सर्व हरियाणा ग्रामीण बैंक
Sarva Haryana Gramin Bank
(भारत सरकार का उपक्रम) (Govt. of India Undertaking)
प्रायोजक : पंजाब नैशनल बैंक Sponsored by: Punjab National Bank

Inspection & Audit Division, Head Office, Plot No. 1, Sector 3, Rohtak-124001
Email: headofficeinspection@gmail.com, hoinspshgb@shgbank.co.in

TO ALL OFFICES **Date: 31.03.2023**

INSPECTION & AUDIT DIVISION
CIRCULAR NO. 11/2023

Reg : KNOW YOUR CUSTOMER (KYC) POLICY, 2023-24.

The KYC Policy of the Bank for the year 2023-24 has been approved by the Board of Bank in its 68th meeting held on 27 March 2023.

For convenience of the field functionaries, a list of *-Frequently Asked Questions (FAQs)*ll has been appended to the Board approved KYC policy at Annexure-IV.

Please note that KYC process and its total compliance must be taken very seriously across all levels at the Bank and serious action be taken and accountability be fixed for non-compliance of KYC guidelines.

The revised KYC Policy is enclosed as Annexure – A, for information, guidance and strict compliance by all the Branches / Offices.

All the inspecting officials are advised to ensure that KYC guidelines are strictly complied with by the branches. Any deviations in this regard should be recorded in the prescribed Risk Based Internal Audit templates/ inspection reports and the observations will be dropped only after verifying proper compliance. Any non- adherence of KYC guidelines and prescribed customer due diligence procedures may lead to money laundering, terrorist financing etc. which may result in operational / reputation loss and penal action(s) against the Bank by regulatory/ statutory authorities.

(Rohit Nijhawan)
General Manager

Annexure 'A'(I & A D Circular No. 11/2023 dated 31.03.2023 refers)

Know Your Customer (KYC) Policy, 2023-24

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India and Aadhaar and other Laws (amendment) Ordinance, 2019 as notified by the Government of India, Bank is required to follow certain customer identification procedure while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions.

This KYC Policy is issued as per RBI's Master Directions on Know Your Customer (updated upto 25.01.2021) which incorporates the amendments made by Government of India, vide Gazette Notification G.S.R. 582(E) dated August 19, 2019 and Gazette Notification G.S.R. 840(E) dated November 13, 2019.

All offices of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

PRELIMINARY

1. Short Title

Policy guidelines on Know Your Customer (KYC) Norms / Anti Money laundering (AML) Standards / Combating of Financing of terrorism (CFT) Measures / Obligation of the Bank under Prevention of Money Laundering Act (PMLA), 2002 shall be called as Know Your Customer (KYC) Policy, 2022.

2. Applicability

The provisions of KYC Policy guidelines shall apply to all the branches / offices of the Bank. Provided this rule shall not apply to 'small accounts'.

3. Definitions

In terms of RBI's Master Direction on KYC, unless the context otherwise requires,the terms herein shall bear the meanings assigned to them below:

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

i. **"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) ofthat section.

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

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

iv. Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of / entitlement to more than 25 per cent of the 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 / 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 chainof control or ownership.

v. **"Certified Copy of OVD"** - Obtaining a certified copy by bank shall mean comparing the copy of 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 under his GBPA/PF no. Branch Official will also attest the duly signed photograph of the

customer.

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

- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.
- Notary Public abroad.

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"** means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

viii. **"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 theBank as per the provisions contained in the Act.

ix. **"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). *[Presently, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 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.

[Presently, as per Information Technology Rules 2016, Rule 9 is related to the manner in which Digital locker System be used by issuer.]

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 8 of the Companies Act, 2013.

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 or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

Further, at the time of on-boarding of the customer, an undertaking should be obtained from the customer along with AOF/OVDs stating that Customer shall submit his OVD with updated current addresswithin 3 months failing which operations in his account shall be restricted.

c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at ‗b' above, failing which the operations in the account shall be restricted (Debit-freezed).

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

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

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

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

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

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

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

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

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

xviii. **A 'Small Account'** means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 18.

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

i. opening of an account;
ii. 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;
iii. the use of a safety deposit box or any other form of safe deposit;
iv. entering into any fiduciary relationship;
v. any payment made or received, in whole or in part, for any contractual

or other legal obligation; or

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

xx.-**UCIC"** means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

xxi. "Video based Customer Identification Process (V-CIP)": a method of customer identification 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. Such process shall be treated as face-to-face process for thepurpose of this KYC Policy.

B. Terms bearing meaning assigned in RBI Master Directions on KYC, unless the context otherwise requires, shall bear the meanings assigned to them below:

a. **"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.

b. **"Customer"** means a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

d. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.

e. **"Customer identification"** means undertaking the process of CDD.

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

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

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

i. **"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.

j. **"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.

k. **"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 politicalparty officials, etc

l. **"Shell bank"** means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

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

n. **"Domestic and cross-border wire transfer":** When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

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

C. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and Aadhaar and other Laws (amendment) Ordinance, 2019', any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

General

4. RBI has advised the Bank that a Know Your Customer (KYC) Policy, duly approved by the Board of Directors of the Bank, be formulated and put in place.

Purpose

5. The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

6. For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

Objective

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

(a) To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.

(b) 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.

8. **The KYC policy includes following four key elements:**

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

9. Designated Director:

a. Bank to nominate an Executive 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. Designated Director shall be nominated by the Board.

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

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

10. Principal Officer:

a. The Board has nominated General Manager, I&A Division as Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information asrequired under the law / regulations.

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

c. The Principal Officer will report to Designated Director through General Manager designated for KYC compliance, who shall be the administrative head of Centralised AML Cell and will oversee the functioning of Centralised AML Cell as per PML Act/ KYC Policy.

d. The Principal Officer will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.

11. Compliance of KYC policy:

a. Bank to ensure compliance with KYC Policy through:

i. A senior officer in the rank of General Manager will constitute as 'Senior Management' for the purpose of KYC compliance.
ii. Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / Regional Office level.
iii. All HO Divisions to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
iv. Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Compliance Division, HO.
v. Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.
vi. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports from EDW / CBS.

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

c. 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 assessmentshould-

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.

d. The implementation of KYC-AML guidelines by branches in letter and spirit, has to be ensured by Regional Managers and the same is to be checked during their visit to branches.

Customer Acceptance Policy

12. Bank to frame a Customer Acceptance Policy. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, Bank shall ensure that:

a. No account is opened in anonymous or fictitious / benami name.
b. No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-

reliability of the documents / information furnished by the customer.

c. No transaction or account based relationship is undertaken without following the CDD procedure.
d. The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
e. 'Optional' / additional information is obtained with the explicit consent of the customer after the account is opened.
f. Bank will apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of Bank desires to open another account with the same Bank, there shall be no need for a fresh CDD exercise.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
h. Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
i. No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
k. 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).

13. Bank to ensure that the 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.

Risk Management

14. For Risk Management, Bank shall have a risk based approach which includes the following.

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

15. It is hereby specified that the various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

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

Customer Identification Procedure (CIP)

16. Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:

a. Commencement of an account-based relationship with the customer.
b. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.
c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
d. Selling third party products as agent, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than rupees fifty thousand.
e. Carrying out transactions for a non-account based customer, that is a walk- in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
f. When 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.
g. Bank shall ensure that introduction is not to be sought while openingaccounts.

17. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank, will at its 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 Bank to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the thirdparty 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 Bank.

Customer Due Diligence (CDD) Procedure

Part I -CDD Procedure in case of Individuals

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

a) the Aadhaar number where,

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

ii. he decides to submit his Aadhaar number voluntarily to 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; and

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

c) one recent photograph; and

d) 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 statue, Complete Income Tax Returns (Not just the acknowledgement) etc. 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 un-organized sector, farmers etc may submit self-declaration to this effect.

Provided that where the customer has submitted,

i. Aadhaar number under clause (a) 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.
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 Bank shall carry out offline verification.

iii. an equivalent e-document of any OVD, the Bank 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 Annexure I.

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

19. Provided that for a period not beyond such date as may be notified by the Government for a class of Banks, 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.

20. 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 or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits his a 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/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, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

21. While establishing an account based relationship with individual customer, the branch official to 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.

22. 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 thecustomer. Branch official will ensure that all the mandatory fields in Account Opening Form / Customer Master Form (marked as *) 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. The respective division/ offices of the Bank shall ensure that branches are capturing correct data in CBS system, particularly in respect of Constitution Code, Profession/ Activity, Occupation, Income/ Turnover etc. as risk category of the customer is assigned on the basis of these parameters.

23. In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain. PAN Card and Voter Identity Card, wherever obtained, be verified on-line through the following websites and a print of on-line verification of the said document be held on record with the relevant AOF:

Name of Documents	Website / Link
PAN Card	Finacle Home Page → Non CBS Applications → GBD → On line PAN verification
Voter Identity Card	www.nvsp.in (National Voters Service Portal)

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

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

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

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

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

(v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 15 is to be carried out

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

(vii) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non- face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank 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 in non-face-to-face mode.

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

(B) Bank may undertake live Video based Customer Identification Process (V-CIP), to be carried out by an official of the Bank, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations.

(i) The official of the Bank performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information either through OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aidingthe V-CIP.

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

(iii) Live location of the customer (Geotagging) shall be captured to ensure that

customer is physically present in India.

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

(v) The official of the Bank shall ensure that the sequence and/or type of questions (to be decided by RBD) during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

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

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

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

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

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

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

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

(xiii) Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 15.

(xiv) BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank. These provisions will be applicable as and when the system/facility is introduced by bank.

(C) Notwithstanding anything contained in Section 15 and as an alternative thereto, in case an individual who desires to open a bank account, banks shall open a Small Account', which entails the following limitations:

(i) the aggregate of all credits in a financial year does not exceed rupees onelakh;

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

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

Provided, that this limit on balance shall not be considered while making deposits through

government grants, welfare benefits and payment against procurements.

(D) Further, small accounts are subject to the following conditions:

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

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

c) 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.

d) 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.

e) 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.

f) 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.

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

h) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per Section 15.

i) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 15.

(E) KYC verification once done by one branch / office of the Bank shall be valid for transfer of the account to any other branch / office of the same Bank, provided full KYC verification has already been done for the concerned account and the sameis not due for periodic updation.

Part II - CDD Measures for Sole Proprietary firms

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

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

(i) Registration certificate
(ii) Certificate / Licence issued by the municipal authorities under Shop and 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 / Licence / certificate of practice issued in the name of the proprietary

concern by any professional body incorporated under a statute.

(vii) 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.

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.

Part III- CDD Measures for Legal Entities

i. **For opening an account of a company,** certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

(i) Certificate of incorporation;

(ii) Memorandum and Articles of Association;

(iii) Permanent Account Number 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) Documents, as specified in Section 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

ii. **For opening an account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

(i) Registration certificate;

(ii) Partnership deed;

(iii) Permanent Account Number of the partnership firm; and

(iv) Documents, as specified in Section 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

iii. **For opening an account of a trust,** certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

(i) Registration certificate;

(ii) Trust deed;

(iii) Permanent Account Number or Form No.60 of the trust; and

(iv) Documents, as specified in Section 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

iv. **For opening an account of an unincorporated association or a body of individuals,** certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:

(i) Resolution of the managing body of such association or body of individuals;

(ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;

(iii) Power of attorney granted to transact on its behalf;

(iv) Documents, as specified in Section 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
(v) 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 underthe term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies.

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

(i) Document showing name of the person authorised to act on behalf of the entity;
(ii) Documents, as specified in Section 15, of the person holding an attorney to transact on its behalf and
(iii) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

vi. **For opening an account of Hindu Undivided Family,** certified copies of each of the following documents shall be obtained :

(i) Identification information as mentioned under Section 15 in respect of the Karta and Major Coparceners,
(ii) Declaration of HUF and its Karta,
(iii) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
(iv) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

Part IV - Identification of Beneficial Owner

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

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

b. In cases of trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Part V - On-going Due Diligence

i. 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.

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

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

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

Explanation: High risk accounts have to be subjected to more intensified monitoring.
a. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
b. The transactions in accounts of marketing firms, especially accounts of Multi- level Marketing (MLM) Companies shall be closely monitored.

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

iv. Periodic Updation

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

a. Bank shall carry out

(i) CDD, as specified in Section 15, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

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

Provided, Bank shall ensure that KYC documents, as per extant requirements of the Master Direction on KYC issued by RBI, are available with them.

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

c. Bank shall ensure to provide acknowledgment with date of having performed KYC updation.

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

e. 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 the KYC documents.

f. 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 which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or the equivalent e-document thereof or Form No. 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.

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

i. **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.

ii. Accounts of Politically Exposed Persons (PEPs)

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

(i) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
(ii) the identity of the person shall have been verified before accepting the PEP as a customer;
(iii) the decision to open an account for a PEP is taken at a senior level, i.e. at the level of Sr. Manager and above, in accordance with the Bank's Customer Acceptance Policy;
(iv) all such accounts are subjected to enhanced monitoring on an on-going basis;
(v) 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. Senior Manager and above is obtained to continue the business relationship;
(vi) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

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

iii. Client accounts opened by professional intermediaries:

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.

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

B. Simplified Due Diligence

iv. Simplified norms for Self Help Groups (SHGs)

a. CDD of all the members of SHG shall not be required while opening savings bank account of SHG.
b. CDD all the office bearers shall suffice.
c.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.

Record Management

v. The 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 dateof transaction;
b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
c. make available the identification records and transaction data to the competent authorities upon request;
d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
e. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following :
(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it wasdenominated;
(iii) the date on which the transaction was conducted; and
(iv) the parties to the transaction.

f. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
g. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

C. Reporting Requirements to Financial Intelligence Unit - India

i. 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.

ii. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Bank in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Bank which are yet to install/adopt suitable technological tools for extracting CTR / STR from their live transaction data.

iii. 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. Bank shall not put any restriction on operations in the accounts where an STR has been filed. Bank 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.

iv. 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.

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

(1) Cash Transaction Report (CTR).

(i) 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.

(ii) The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

(iii) A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through RPT1 Report: RPT1-30 & 31) for production to auditors/Inspectors, when asked for.

(2) Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, bank will be guided by the definition of —suspicious transaction‖ 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:

a. gives rise to a reasonable ground of suspicion that it may involveproceeds 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 involvefinancing 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.

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

(iii) 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.

(iv) 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.

(v) 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.

(vi) 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 controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular.

(vii) For effective monitoring of transactions of the customers, Bank has implemented an AML system for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. Further, an indicative list of behavioral/observation based scenarios has been circulated vide KYC AML Division Circular no. 10/2018 dated 04.06.2018. In case any suspicious transaction is detected, the same be reported to Centralised AML Cell for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FINnet Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring, high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at **Annexure-II**.

(3) Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or 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.

(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.

(5) Cross-border Wire Transfer [CWTR]

Bank will file Cross-Border Wire Transfer Report (CWTR) to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is inIndia.

E. Internal Control System

i. At each Regional Office, an Officer in the rank of Sr. Manager / Chief Manager be designated as Nodal Officer for compliance of KYC Policy in all Offices under its jurisdiction.

ii. **Dy. Money Laundering Reporting Officer (DMLRO) cum Regional Compliance Officer (DMLRO cum RCO):** At each Regional Office, an Officer, not below the rank of Sr. Manager, shall be designated as DMLRO cum RCO, who would be responsible for compliance of KYC Policy in all the branches under the allotted Regional Office. He will prepare STRs pertaining to local adverse media reports, Law Enforcement Agency enquiries, public complaints, behavioral scenarios, attempted transactions etc. in all the branches under allotted Regional Office and will send STRs to Centralized AML Cell. Similarly, if during execution of his duties, DMLRO cum RCO observes any money laundering activity at BO/RO, he will escalate the same to Centralized AML Cell. DMLRO-cum-RCO to ensure that field functionaries are sensitized on KYC / AML guidelines and ensure that no money laundering activities take place in the branches under his/her jurisdiction. For this purpose he/she should also ensure on-site supervision by visiting the branches under his/her jurisdiction for random checking of compliance of KYC/ AML guidelines of the Bank.

iii. **Centralized AML Cell:** Monitoring, analysis & closure of AML alerts, including Trade Based Money Laundering (TBML) alerts, shall be done at Centralized AML Cell on day to day basis. Makers/ Checkers at Centralized AML Cell will analyze alerts pertaining to their respective assigned Regions on day to day basis and will close the alerts after thorough analysis of the transactions / alerts and ensuring that all the transactions are genuine in nature & match with the business profile of customers. Post-closure scrutiny of closed alerts (@10%) shall be undertaken at Centralized AML Cell by officers upto Scale-III. Further, Chief Managers at Centralized AML Cell will also review / scrutinize at-least 5% of the closed alerts, pertaining to their respective Regions, on sample basis. They will also ensure that necessary corrective steps are initiated for the discrepancies observed during sample checking.
STRs on all suspicious transactions shall be put up to Principal Officer immediately for approval and onward submission to FIU-IND. Similarly, STRs on adverse media reports, Law Enforcement

Agency enquiries etc. shall also be prepared and put up to Principal Officer.

During analysis of alerts, special attention shall be given to alerts pertaining to TBML, High Risk Customers, Politically Exposed Persons & High Value Transactions.

iv. Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members. Senior Officers from the Regional/Head Offices, during their visits to the branches will ensure that KYC / AML guidelines are being strictly adhered to as per the laid down procedures, keeping in view the risk involved in a transaction, accountor banking/business relationship.

v. For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data
and other Customer Due Diligence information, transaction records and otherrelevant information.

vi. Any changes in KYC Policy may be implemented after approval of the Board.

F. Requirements / Obligations under International Agreements

Communications from International Agencies

i. Bank 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.

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 March 14, 2019.

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.

G. Freezing of Assets under of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated March 14, 2019 (Annexure- III of this KYC Policy) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

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

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

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

Explanation: The process referred to in Section 51 a & b do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

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

H. <u>Other Instructions</u>

i. Secrecy Obligations and Sharing of Information:

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

b. While considering the requests for data / information from Government and other agencies, bank 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.

c. 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.

d. 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

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

Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities'

as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015. The 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 within ten days of opening the accounts.

iii. 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.

iv. 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.

v. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shallnot be collected.

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

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

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

viii. Correspondent Banks

Correspondent banking is the provision of banking services by one bank (the ―correspondent bank) to another bank (the ―respondent bank). These services include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc.

Bank will have a policy approved by the Board, or by a committee headed by the Chairman / CEO / MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

a. Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/ CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory / supervisory framework in the bank's home country shall be gathered.
b. The accounts of the respondent banks will be opened with the prior approval of International Banking Division, Head Office, who would also be doing the due diligence in terms of the guidelines issued by RBI and Govt. of India. Similarly, IBD, HO will complete due diligence requirements in correspondent banking relationships where Bank is availing correspondent banking services from other banks.
c. Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.
d. The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
e. In the case of payable-through-accounts, the Bank shall satisfy that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on- going 'due diligence' on them.
f. The Bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
g. Correspondent relationship shall not be entered into with a shell bank (i.e. a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).
h. It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.
i. Bank will be cautious with respondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
j. Bank will ensure that respondent banks have KYC / AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

ix. Wire transfer

Bank shall ensure the following while effecting wire transfer:
a. All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.
b. Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.
c. Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.
d. Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.
e. Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.
f. A bank processing as an intermediary element of a chain of wire transfers shall ensure

that all originator information accompanying a wire transfer is retained with the transfer.

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

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

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

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

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

x. Issue and Payment of Demand Drafts, etc.

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

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

xi. 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.

xii. Selling Third party products

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

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

b. transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 39.

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

i. transactions involving rupees fifty thousand and above shall be undertaken only by:

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

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

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

a. The 'at par' cheque facility offered by Bank 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 Bank.

xiv. Issuance of Prepaid Payment Instruments (PPIs) :

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

xv. 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 Bank, regulation and related issues shall be ensured.

Annexure-I

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 its 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 Bank 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 watermark 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/ eAadhaar 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 Bank shall check and verify that:-

a information available in the picture of document is matching with the information entered by authorized officer in CAF.

b live photograph of the customer matches with the photo available in the document.; and

c 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 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.

Annexure – II

INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS I.E. CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING, HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/ LOCATIONS/ALERTS FOR BRANCHES/ OFFICES

1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

i. 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.
ii. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
iii. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
iv. Customer giving confusing details about a transaction.
v. 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.
vi. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
vii. 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.
viii. Customer‘s representatives avoiding contact with the branch.
ix. Customers who repay the problem loans unexpectedly.
x. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
xi. 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.
xii. Customer regularly issues large value cheques without balance and then deposits cash.
xiii. Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions Involving Large Amounts of Cash

i. Exchanging an unusually large amount of small denomination notes forthose of higher denomination;
ii. Purchasing or selling of foreign currencies in substantial amounts bycash settlement despite the customer having an account with the bank;
iii. Frequent withdrawal of large amounts by means of cheques, includingtraveller'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, e.g. 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 whichis substantial.

B. Transactions that do not make Economic Sense

i. A customer having a large number of accounts with the same 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.

C. 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 & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnectedwith 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.

D. 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 that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.

iii. An account where there are several cash deposits/withdrawals below a specified threshold level to a 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 thepurpose of avoiding the threshold limit.

E. 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/centers, which are known for money laundering.

F. Customer who provides Insufficient or Suspicious Information

i. 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.
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.

G. 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 centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. 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.

I. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knowsthe true identity of the account holder.

J. Some examples of suspicious activities/transactions to be monitoredby the operating staff-

i. Large Cash Transactions
ii. Multiple accounts under the same name
iii. Frequently converting large amounts of currency from small to large denomination notes
iv. Placing funds in term Deposits and using them as security for moreloans.
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 thirdParties
ix. Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
x. Cheques of third parties into the account followed by immediate cash withdrawals.
xi. Transactions inconsistent with the purpose of the account.
xii. Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

i. 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).

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 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 wiretransfers to another city or country.

v. A customer experiences increased wire activity when previously there has been no regular wire activity.

vi. Loan proceeds unexpectedly are wired or mailed to an offshore Bank orthird party.

vii. 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.

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 transfers 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 lakhs), the amount is just under a specified threshold, the funds come from a foreign country or such transactions occur repeatedly.

xvii. 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)

xviii. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

2. INDICATIVE LIST OF HIGH RISK CUSTOMERS

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
ii. 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
iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
iv. Customers with dubious reputation as per public information locally available or commercially available.
v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
vi. 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 institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
viii. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
ix. Non-resident customers and foreign nationals
x. Accounts of Embassies / Consulates;
xi. Off-shore (foreign) corporation/business
xii. Non face-to-face customers
xiii. High net worth individuals [HNIs]
xiv. Firms with 'sleeping partners'
xv. Companies having close family shareholding or beneficial ownership
xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
xvii. 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
xviii. Investment Management / Money Management Company/Personal Investment Company
xix. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
xx. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
xxi. Trusts, charities, NGOs/NPOs (especially those operating on a ―cross- border‖ basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
xxii. Money Service Business: including seller of: Money Orders / Travelers" Checks / Money Transmission /Check Cashing / Currency Dealing or Exchange
xxiii. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
xxiv. Gambling/gaming including ―Junket Operators‖ arranging gambling tours
xxv. 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).

xxvi. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
xxvii. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
xxviii. Customers that may appear to be Multi-level marketing companies etc.

3. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

i. Non-Bank Financial Institution
ii. Stock brokerage
iii. Import / Export
iv. Gas Station
v. Car / Boat / Plane Dealership
vi. Electronics (wholesale)
vii. Travel agency
viii. Used car sales
ix. Telemarketers
x. Providers of telecommunications service, internet café, IDD callservice, phone cards, phone center
xi. Dot-com company or internet business
xii. Pawnshops
xiii. Auctioneers
xiv. Cash-Intensive Businesses such as restaurants, retail shops, parkinggarages, fast food stores, movie theaters, etc.
xv. Sole Practitioners or Law Firms (small, little known)
xvi. Notaries (small, little known)
xvii. Secretarial Firms (small, little known)
xviii. Accountants (small, little known firms)
xix. Venture capital companies

4. LIST OF HIGH / MEDIUM RISK PRODUCTS & SERVICES

i. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), etc
ii. Electronic banking
iii. Private banking (domestic and international)
iv. Trust and asset management services
v. Monetary instruments such as Travelers' Cheque
vi. Foreign correspondent accounts
vii. Trade finance (such as letters of credit)
viii. Special use or concentration accounts
ix. Lending activities, particularly loans secured by cash collateral andmarketable securities
x. Non-deposit account services such as Non-deposit investmentproducts and Insurance
xi. Transactions undertaken for non-account holders (occasional customers)

xii. Provision of safe custody and safety deposit boxes
xiii. Currency exchange transactions
xiv. Project financing of sensitive industries in high-risk jurisdictions
xv. Trade finance services and transactions involving high-risk jurisdictions
xvi. Services offering anonymity or involving third parties
xvii. Services involving banknote and precious metal trading and delivery
xviii. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/COUNTRIES

Countries/Jurisdictions

i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions (–UNSCR‖).
ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf- gafi.org)
iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.
vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
vii. Countries identified by credible sources as having significant levels of criminal activity.
viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations

i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

5. INDICATIVE LIST OF HIGH RISK COUNTRIES:

The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

Annexure-III

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

New Delhi, dated 14 March 2019

ORDER

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

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

"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 beengaged in terrorism;
(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism:
(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

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

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order. 2007, as may be amended from time to time. In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide this Ministry Order No. 17015/10/2002-IS-VI dated 27.08.2009. After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR Division. The order dated 27.8.2009 is accordingly modified as under:

Appointment and communication of details of UAPA Nodal Officers

2. As regards appointment and communication of details of UAPA Nodal Officers-

(i) The UAPA Nodal Officer for CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.in (e-mail id).

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

(iii) The States and UTs should appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the CTCR Division in MHA.

(iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.

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

(vi) The consolidated list of the UAPA Noda! Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

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

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

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

(iii) The CTCR Division of MHA would forward the designated lists to the UAPA Nodal Officer of all States and UTs.

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

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

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

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

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

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

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

(v) The banks, stock exchanges /depositories, intermediaries regulated by SEBI and insurance companies, shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 4(ii) above, CTCR Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals / entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these assets under Section 51A of the UAPA would be issued by the UAPA Nodal Officer of CTCR Division of MHA and conveyed electronically/to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA Nodal Officer of CTCR Division of MHA shall also forward a copy thereof to ail the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of CTCR Division of MHA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual/entity.

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

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

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found. The UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to Joint Secretary (CTCR), Ministry of Home Affairs, immediately within 24 hours at Fax No.011- 23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id jsctcr- mha@gov.in.

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

10. A copy of this reference should be sent to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also conveyed over telephone on 01123092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: jsctcr-mha@gov.in. MHA may also have the verification conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under section 51A of the UAPA would be issued, by the UAPA Nodal Officer of CTCR Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.

    The order shall be issued without prior notice to the designated individual/entity.

12. Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State / UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State / UT for also initiating action under the provisions of Unlawful Activities (Prevention)Act 1967.

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

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons: and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property

owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

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

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

16. Upon receipt of the requests by these Nodal Officers from the UAPA nodal officer of CTCR Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

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

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

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

18. The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been

frozen inadvertently, to the Nodal Officer of CTCR Division of MHA as per thecontact details given in paragraph 4 (ii) above, within two working days.

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

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act, 1967.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 relating to funds, financial assets or economic resources or related services, would be communicated to all the banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all Registrars performing the work of registering immovable properties, through the State/UT Nodal Officer by CTCR Division of MHA.

Regarding prevention of entry into or transit through India

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

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

Procedure for communication of compliance of action taken under section51A

23. The Nodal Officers of CTCR Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

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

(Piyush Goyal)

Joint Secretary to the Government of India

1. Governor, Reserve Bank of India, Mumbai
2. Chairman, Securities & Exchange Board of India, Mumbai
3. Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4. Foreign Secretary, Ministry of External Affairs, New Delhi.
5. Finance Secretary, Ministry of Finance, New Delhi.
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7. Director, Intelligence Bureau, New Delhi.
8. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
9. Chief Secretaries of all States/Union Territories
10. Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
11. Directors General of Police of all States & Union Territories
12. Director General of Police, National Investigation Agency, New Delhi.
13. Commissioner of Police, Delhi.
14. Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
15. Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance. New Delhi.
16. Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, NewDelhi.
17. Director (FIU-IND), New Delhi.

Annexure-IV

FREQUENTLY ASKED QUESTIONS (FAQs)

Q 1. What is KYC?
Response: KYC is an acronym for ―Know your Customer‖ a term used for Customer identification process. It is a process by which banks obtain information about the identity and address of the customers 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.

It involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, financial status & nature of customer's business, reasonableness of operations in the account in relation to the customer's overall profile, etc. which in turn helps the banks to manage their risks prudently.

Q 2. What is the objective of KYC?
Response: The objective of the KYC guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities.

KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently and 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.

Q 3. What is Money Laundering and Terrorist financing?
Response: Money laundering refers to conversion of money illegally obtained to make it appear as if it originated from a legitimate source. Money laundering is being employed by launderers worldwide to conceal criminal activity associated with it such as drugs /arms trafficking, terrorism and extortion. Terrorist financing means financial support to, in any form of terrorism or to those who encourage, plan or engage in terrorism. Money launderers send illicit funds through legal channels in order to conceal their criminal origin while those who finance terrorism transfer funds that may be legal or illicit in original in such a way as to conceal their source and ultimate use, which is to support Terrorist financing.

Money laundering has become a pertinent problem worldwide threatening the stability of various regions by actively supporting and strengthening terrorist networks and criminal organizations. The links between money laundering, organized crime, drug trafficking and terrorism pose a risk to financial institutions globally. Government of India has promulgated Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and RBI Master Direction on KYC, enforces legal/statutory/regulatory obligations on both bank and customers to provide KYC information/documents.

Q 4. Whether KYC is mandatory?

Response: Yes. It's a regulatory and legal requirement.

- Regulatory: - In terms of the guidelines issued by the Reserve Bank of India (RBI) on 29 November, 2004 on Know Your Customer (KYC) Standards - Anti Money Laundering (AML) measures, all banks are required to put in place a comprehensive policy framework covering KYC Standards and AML Measures.
- Legal:- The Prevention of Money Laundering Act, 2002 (PMLA) which came into force from 1st July, 2005 (after ―rules‖ under the Act were formulated and published in the Official Gazette) also requires Banks, Financial Institutions and Intermediaries to ensure that they follow certain minimum standard of KYC and AML as laid down in the ACT and the ―rules‖ framed thereunder.

Q 5. Is KYC information obtained from customer kept confidential?

Response: Yes, the customer profile/information collected by the Bank at the time, of account opening or otherwise, are kept confidential and are not disclosed to any person, except when required under the provisions of applicable laws and regulations or where there is a duty to the public to disclose or the interest of bank requires disclosure.

Q 6. What are the documents to be obtained from customers as 'proof of identity' and 'proof of address'?

Response: The Government of India has notified six documents or its equivalent e-documents as 'Officially Valid Documents (OVDs) for the purpose of producing proof of identity of individual customers. These six documents are the passport, the driving license, 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.

You need to submit any one of these documents as proof of identity. If these documents also contain your current address details, then it would be accepted as 'proof of address'. Provided that if customer is desirous of receiving any benefit or subsidy under any scheme notified under Aadhaar Act, 2016, customer shall be required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

KYC documents to be obtained from non-individual customers have been specified in the KYC policy.

Q 7. If customer do not have any of the OVDs listed above with current updated address, can customer provide other OVD?

Response: Yes, customer can provide the following documents or the equivalent e-documents for the limited purpose of proof of address, with an undertaking along with AOF/OVDs stating that he/she shall submit his OVD with updated current address within 3 months failing which operations in his/her account shall be restricted.

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- Property or Municipal tax receipt;
- Pension or family pension payment orders (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 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.

However, if customer undertakes Aadhaar authentication using e-KYC facility of UIDAI and 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.

Q 8. Are there any additional documents to be obtained from customer apart from 'proof of identity' and 'proof of address'?
Response: Yes, atleast one document in support of the declared Profession / activity, nature of business, financial status, annual income/ turnover (in case of business) has to obtained from individual customers; 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 statue, Complete Income Tax Returns (Not just the acknowledgement) etc.

Q 9. What if the customer doesn't have any document in support of nature of business, financial status, annual income?
Response: Customers who don't have any business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in un-organized sector, farmers etc may submit self-declaration to this effect.

Q 10. If customer does not have any of the documents listed above to show his/her 'proof of identity', can he/she still open a bank account?
Response: Yes, customer can still open a bank account known as 'Small Account', which entails certain limitations, by submitting his/her recent photograph and putting signature or thumb impression in the presence of a bank official.

Q 11. Is there any difference between such 'small accounts' and otheraccounts?
Response: Yes. The 'Small Accounts' have certain limitations such as:

- balance in such accounts at any point of time should not exceed ₹50,000
- total credits in one financial year should not exceed ₹1,00,000
- total withdrawal and transfers should not exceed ₹10,000 in a month.
- Foreign remittances cannot be credited to such accounts.

Such accounts 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 bank of having applied for any of the officially valid documents within twelve months of the opening of such account. The bank will review such account after twenty four months to see if it requires such relaxation.

Q 12. If customer refuses to provide requested documents for KYC to the bank for opening an account, what may be the result?
Response: If customer does not provide the required documents for KYC, the bank shall not open the account.

Q 13. Can a customer open bank account with only an Aadhaar card? Response: As per RBI directions, Aadhaar card is now accepted as a proof of both, identity and address. However, PAN/Form 60 along with one document or the equivalent e-document thereof in

support of the declared Profession / activity, nature of business or financial status is also required.

Q 14. Is Aadhaar mandatory for opening of an account?
Response: No, Aadhaar is not mandatory for opening of an account. As per RBI directions, only an individual who 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) is mandatorily required to provide Aadhaar and is required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

Q 15. What is e-KYC? How does e-KYC work?
Response: e-KYC refers to electronic KYC. e-KYC is possible only for those who have Aadhaar number or proof of possession of Aadhaar. While using e-KYC service, customer has to authorise the Unique Identification Authority of India (UIDAI), by explicit consent, to release his/her identity/address through biometric authentication to the bank branches/business correspondent (BC). The UIDAI then transfers his/her data comprising name, age, gender, and photograph of the individual, electronically to the bank/BC. Information thus provided through e-KYC process is permitted to be treated as an 'Officially Valid Document' under PMLRules and is a valid process for KYC verification.

Q 16. Is introduction necessary while opening a bank account?
Response: No, introduction is not required.

Q 17. Can a customer transfer his existing bank account from one branch to another?
Response: KYC verification once done by one branch / office of the Bank shall be valid for transfer of the account to any other branch / office of the same Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Q 18. Is a customer required to furnish KYC documents for each accounthe/she opens in the Bank?
Response: As per RBI guidelines, an individual customer can maintain only a single Unique Customer ID Code (UCIC)/Customer-ID in a Bank and all the accounts of the customer have to be opened/ linked under this Customer-ID. Therefore, if a customer has opened an account with the Bank, which is KYC compliant, then for opening another account, furnishing of documents is not necessary.

Q 19. Customer's KYC was completed when he/she opened the account. Why does Bank ask for doing KYC again?
Response: In terms of RBI guidelines, Bank is required to periodically update KYC records. This is a part of ongoing due diligence on bank accounts. The periodicity of such updation varies from account to account or categories of accounts depending on the Bank's perception of risk. Further, the Bank may insist for KYC updation, whenever there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

Q 20. What are the rules regarding periodical updation of KYC?
Response: Different periodicities have been prescribed for updation of KYC records depending on the risk perception of the bank. Periodic updation of KYC is to 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. Bank has to review the

documents sought at the time of opening of account and obtain fresh certified copies from customer. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect may be obtained.

Provided Bank has to ensure that KYC documents, as per extant requirements of the Master Direction, are available with the Bank.

Q 21. What if the customer does not provide KYC documents at the time of periodic updation?
Response: If customer does not provide his/her KYC documents at the time of periodic updation, Bank shall temporarily cease operations in the account. The account holders shall have the option to revive their accounts by submitting the KYC documents.

Q 22. Do the customer need to submit KYC documents to the bank while purchasing third party products (like insurance or mutual fund products) frombanks?
Response: Yes, all customers who do not have accounts with the Bank (known as walk-in customers) have to produce proof of identity and address while purchasing third party products from Bank if the transaction is for ₹50,000 and above. KYC exercise may not be necessary for bank's own customers for purchasing third party products. However, instructions to make payment by debit to customers' accounts or against cheques for remittance of funds/issue of travellers' cheques, sale of gold/silver/platinum and the requirement of quoting PAN number for transactions of ₹50,000 and above would be applicable to purchase of third party products from Bank by Bank's customers as also to walk-in customers.