International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022

(Updated as on January 02, 2026)

TABLE OF CONTENTS

INDEX OF ABBREVIATIONS

Sl. No.	Abbreviation	Full form
1.	AML/CFT	Anti-Money Laundering/Countering of Terrorist Financing (also used for *Combating the financing of terrorism*)
2.	BF	Business facilitator
3.	BO	Beneficial Owner
4.	CDD	Customer Due Diligence
5.	CKYCR	Central Know Your Customer Records Registry
6.	CRS	Common Reporting Standards
7.	ECDD	Enhanced Customer Due Diligence
8.	FATCA	Foreign Account Tax Compliance Act
9.	FATF	Financial Action Task Force
10.	FIU-IND	Financial Intelligence Unit- India
11.	IFSCs	International Financial Services Centres
12.	IFSCA	International Financial Services Centres Authority
13.	KYC	Know Your Customer
14.	KRA	KYC Registration Agency
15.	ML/TF	Money Laundering/Terrorist Financing
16.	NPO	Non-Profit Organisation
17.	NRI	Non- Resident Indian
18.	NTR	Non-Profit Transaction Report

19.	OVD	Officially Valid Document
20.	PEP	Politically Exposed Person
21.	RBA	Risk-Based Approach
22.	RE	Regulated Entity
23.	SCDD	Simplified Customer Due Diligence
24.	STR	Suspicious Transaction Report
25.	V-CIP	Video- Customer Identification Procedure
26.	UAPA	Unlawful Activities (Prevention) Act, 1967
27.	UNSC	United Nations Security Council
28.	WMD	Weapons of Mass Destruction

CHAPTER – I

APPLICABILITY, DEFINITIONS AND DUTIES OF A REGULATED ENTITY

1.1. Short title and commencement

These Guidelines may be called as International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022, and shall come into force from the date of its publication in the official gazette[1].

1.2. Applicability

1.2.1. [2][Save as otherwise provided under clause 1.2.3., the provisions of these Guidelines shall apply to every Regulated Entity which is licensed, recognized, registered or authorized by the Authority.

Provided that the Authority may exempt any activity or a Regulated Entity from the applicability of these Guidelines.]

1.2.2. The provisions of these Guidelines shall also apply to a Financial Group of the Regulated Entity, to such extent as specified in Chapter-XII.

1.2.3. [3][The following entities or activities shall be exempted from the applicability of these Guidelines:

i. Global-in-House Centre' registered under IFSCA (Global In-House Centres) Regulations, 2020;

ii. 'International Branch Campus' ("IBC") or an 'Offshore Educational Centre' ("OEC") of a Foreign University or a Foreign Educational Institution registered

[1] Vide Gazette Notification No. IFSCA/2022-23/GN/GL001 dated 28th October 2022, published in the Gazette of India, Extraordinary, Part III, Sec.4, vide No. 533 on 31st October 2022.
[2] Substituted for "The provisions of these Guidelines shall apply to every Regulated Entity which is licensed, recognized or registered by International Financial Services Centres Authority (IFSCA) and also to the Regulated Entities authorized by it, to the extent specified." vide Circular dated January 02, 2026.
[3] Clarified vide Circular dated November 18, 2024 (the circular can be accessed at: https://shorturl.at/XCzX2)

under IFSCA (Setting up and Operation of International Branch Campuses and Offshore Education Centres) Regulations, 2022;

iii. 'Financial Crime Compliance Services Provider' registered under IFSCA (Book-keeping, Accounting, Taxation and Financial Crime Compliance Services) Regulations, 2024; and

iv. A Financial Institution providing services only to the entities in its 'Financial Group' which are located in a country not identified in the public statement of FATF as '*High-risk jurisdictions subject to call for action'*.

Provided that, any financial institution undertaking transactions through third-party business / service providers in the course of their operations, shall undertake business risk assessment and comply with incidental provisions of the Guidelines.

1.2.4. The entities exempted in clause 1.2.3. shall undertake Business Risk Assessment and document the same. In the event any AML/CTF risk are envisaged in the business risk assessment, such entities shall continue to comply with the provisions of the Prevention of Money Laundering Act, 2002 and Rules made thereunder, and these Guidelines.]

1.3. Definitions

In these Guidelines, unless the context otherwise requires, -

1.3.1. "Act" and "Rules" means the Prevention of Money-laundering Act, 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, respectively.

1.3.2. "Authority" or "IFSCA" means the International Financial Services Centres Authority established under sub-section (1) of section 4 of International Financial Services Centres Authority Act, 2019 (50 of 2019).

1.3.3. "Beneficial Owner" means: -

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

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of or entitlement to more than [4][ten] per cent. of the shares or capital or profits of the company;

[4] Substituted for "twenty-five" vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).

(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 [5][ten] per cent. of capital or profits of the partnership [6][or who exercises control through other means.

Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decision;]

(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 or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (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 [7][ten] per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Explanation: - For the purpose of determination of beneficial owner, any amendment made under sub-rule 3 of rule 9 of Rules, shall be applicable in addition to the requirements under these Guidelines.

1.3.4. "Beneficiary Institution" means the financial institution that receives the wire transfer from the ordering institution, directly or through an intermediary institution, and makes the funds available to the wire transfer beneficiary.

1.3.5. "Business Facilitator" means a person authorised by the Regulated Entity, to verify the information/officially valid documents provided by the customer for opening account

[5] Substituted for "fifteen" vide Circular dated September 8, 2023 (the Circular can be accessed at https://shorturl.at/MwsLx).
[6] Inserted vide Circular dated September 8, 2023 (the Circular can be accessed at https://shorturl.at/MwsLx).
[7] Substituted for "fifteen" vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).
.

with it.

1.3.6 "Central KYC Records Registry" means an entity defined under rule 2 (1) (ac) of the Rules, which is authorised to receive, store, safeguard and retrieve the KYC records of a customer in digital form.

1.3.7. "Certified Copy" means comparing the original officially valid document provided by the customer with the copy thereof and recording the same as 'true copy' by the authorised officer of the Regulated Entity.

Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by:

(i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;

(ii) Notary Public (outside India);

(iii) Court Magistrate (outside India);

(iv) Judge (outside India);

(v) Certified public or professional accountant (outside India);

(vi) Lawyer (outside India);

(vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or

(viii) Any other authority as may be specified by the Authority.

1.3.8. "Common Reporting Standards" 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.

1.3.9. "Cover payment" means a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction (the cover) from the ordering institution to the beneficiary institution through one or more intermediary institutions.

1.3.10. "Cross-border wire transfer" means any wire transfer (including a chain of wire transfers) where either the ordering institution or the beneficiary institution is located in IFSC.

1.3.11. "Customer" or "Client" for the purpose of these Guidelines shall mean a person who is engaged in a financial transaction or activity with a Regulated Entity and includes a person on whose behalf the person engaged in the transaction or activity, is acting.

1.3.12. "Designated Director" means a person designated by the Regulated Entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules

and these Guidelines.

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

1.3.14. "Digital Signature" shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

1.3.15. "Domestic Wire Transfer" means a wire transfer where both the ordering institution and beneficiary institution are located in the IFSC and also refers to any chain of wire transfers that takes place entirely within the IFSC.

1.3.16. "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 or its equivalent in other jurisdictions, as may be recognised by the Authority.

1.3.17. "FATCA" means Foreign Account Tax Compliance Act, 2010 of the United States of America (USA) which, inter-alia, requires reporting 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.

1.3.18. "Financial Group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

1.3.19. "Financial Intelligence Unit – India" refers to a national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions.

1.3.20. "Governing Body" means:

(a) In relation to a company- the board of directors;

(b) In relation to a partnership firm- the partner(s);

(c) In relation to a limited liability partnership- the partners including any designated partner (s);

(d) In relation to a trust- the managing trustee (s); and

(e) In relation to an unincorporated association or a body of individuals - committees of management or anybody who controls and manages the affairs of such unincorporated association or a body of individuals (consisting of more than one person);

(f) In relation to a Regulated Entity established as a branch, a committee constituted at the branch level with the authorization of the Governing Body of the parent entity of the Regulated Entity.

1.3.21. "International Financial Services Centre" shall have the meaning assigned to it under clause (g) of sub-section (1) of Section 3 of the IFSCA Act, 2019 (50 of 2019).

1.3.22. "Intermediary Institution" means the financial institution in a serial payment or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution.

1.3.23. "International Organisation PEP" means a person who is or has been entrusted with prominent function by an international organisation.

Explanation: This may include members of Senior Management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors and members of the board or equivalent functionaries. An international organisation includes any organisation set up either by the governments of more than one country or by international organisation(s).

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

[8][1.3.24A. "KYC Registration Agency (KRA)" means an entity which has been granted certificate of registration under the International Financial Services Centres Authority (KYC Registration Agency) Regulations, 2025.]

1.3.25. "Money Laundering" shall have the meaning assigned to it under section 3 of the Act and "Anti-Money Laundering" shall be construed accordingly, and shall include Counter-Terrorist Financing and other related measures.

1.3.26. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Regulated Entity or meeting the authorised officials/persons of the Regulated Entity.

1.3.27. "Non-profit organisations" means any entity or organisation[9][, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43

[8] Inserted vide Circular dated January 02, 2026.
[9] Clarified vide Circular dated May 23, 2023. (the Circular can be accessed at https://shorturl.at/APtcZ).

of 1961),] that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a company registered under section 8 of the Companies Act, 2013 (18 of 2013) or other legal entity from any other jurisdictions, which is engaged in not-for-profit activities, and is recognised as such by the Authority.

[10]*[Explanation:* Every Regulated Entity in the form of Banking Unit, Financial Institution or Intermediary, as the case may be, shall register the details of a client, in case of client being a non-profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of [11][five years] after the business relationship between a client and the aforementioned entity has ended or the account has been closed, whichever is later.

For avoidance of doubts, it is clarified that, the definition of 'Financial Institution' and 'Intermediary' shall have the meaning as defined under the section 2(1)(l) and 2(1)(n) respectively, of the Act.]

1.3.28. "Non- Resident Indian" shall have the meaning as defined in Foreign Exchange Management (Deposit) Regulations, 2016.

1.3.29. "Ordering Institution" means the financial institution that initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the wire transfer originator.

1.3.30. "Officially Valid Document" means the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card issued by the Election Commission of India or letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator;

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

[10] Clarified vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).
[11] Inserted vide Circular dated January 02, 2026.

Provided further that, where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be 'officially valid document': -

(a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

(b) letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided also that,

where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document [12] [or the equivalent e-documents thereof] shall also be deemed to be Officially Valid Document:

(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, Municipal tax receipt, [13][*] or such other equivalent document;

(iii) Post Office savings bank account statement or statement of a bank account including of a foreign bank;

(iv) pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

(v) letter of allotment of accommodation from employer issued by State 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; and

Provided also that in case the Officially Valid Document 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;

Provided also that where the client submits his proof of possession of Aadhaar number

[12] Inserted vide Circular dated January 02, 2026.
[13]The words "city council tax receipt," omitted vide Circular dated June 05, 2025 (the Circular can be accessed at https://shorturl.at/4BrTr).

as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.

Explanation: For the purpose of this Clause, a document shall be deemed to be an Officially Valid Document 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.

1.3.31. "Person" means and includes:

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

1.3.32. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the Customer Due Diligence process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity specified by the Authority.

1.3.33. "Principal Officer" means an officer designated by the Regulated Entity as such, who shall be responsible for furnishing information as required under rule 8 of the Rules.

1.3.34. "Politically Exposed Person" means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

Explanation: The definition of Politically Exposed Person is not intended to cover middle ranking or more junior individuals in the definition.

1.3.35. "Regulated Entity" means a unit/entity which has been granted license, recognition, registration or authorisation by the Authority.

1.3.36. "Senior Management" means:

(a) In relation to a Regulated Entity,
  (i) for an incorporated entity in International Financial Services Centre in India, every member of the Regulated Entity's Governing Body;
  (ii) for a branch, the person or persons who control the day-to-day operations of the

Regulated Entity in an IFSC and may include such other persons as may be designated by the Regulated Entity.

(b) In relation to a customer, that is a legal person, every member of its Governing Body and the person or persons who control its day-to-day operations.

1.3.37. "Serial Payment" means a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution, directly or through one or more intermediary institutions.

1.3.38. "Shell financial institution" means a bank or financial institution incorporated, formed or established in a country or jurisdiction where the bank or financial institution has no physical presence, and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

[14][*Explanation:* Physical presence means meaningful mind in the form of senior management located within an IFSC. The existence simply of a local agent or low-level staff does not constitute physical presence.]

1.3.39. "Straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention.

1.3.40. "Suspicious Transaction" means a "Transaction" as defined in these Guidelines, including an attempted transaction, which to a person acting in good faith-

(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

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

(c) appears to have no economic rationale or *bona-fide* purpose; or

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

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

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

(a) opening of an account;

(b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether by payment order or other instruments or by electronic or other non-physical means;

[14] Inserted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).

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

(d) entering into any fiduciary relationship;

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

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

1.3.42. "Unique transaction reference number" means a combination of letters, numbers or symbols, determined by the payment service provider in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer, which permits the traceability of the wire transfer.

1.3.43. "Video based Customer Identification Process" or "V-CIP" means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the Regulated Entity [15][or financial group entity in India supervised by a financial regulator or a KRA Registration Agency], by undertaking seamless, secure, live, informed &consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

Explanation: - Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face customer identification procedure for the purpose of these Guidelines.

1.3.44. "Wire Transfer" means any transaction carried out on behalf of a Wire Transfer Originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a Beneficiary Institution, irrespective of whether the originator and the beneficiary are the same person.

1.3.45. "Wire Transfer Beneficiary" means the natural person, legal person or legal arrangement who is identified by the wire transfer originator as the receiver of the wire transfer funds.

1.3.46. "Wire Transfer Originator" means the account holder who allows the wire transfer from that account; or where there is no account, the natural person, legal person or legal arrangement that places the wire transfer order with the ordering institution to perform the wire transfer.

1.4. Words and expressions used but not defined in these Guidelines shall have the same meaning as assigned to them under the International Financial Services Centres Authority

[15] Inserted vide Circular dated October 31, 2025.

Act, 2019, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

1.5. Duties of a Regulated Entity

(a) Every Regulated Entity shall formulate an AML-CFT policy, which shall be duly approved by the Governing Body or by a committee to whom such power has been delegated by the Governing Body. While formulating the AML-CFT policy, every Regulated Entity shall incorporate the key principles or elements of these Guidelines.

(b) Additionally, every Regulated Entity shall develop a KYC Policy which shall be the part of its AML-CFT policy.

(c) Every member of Regulated Entity's Senior Management shall be responsible for the Regulated Entity's compliance under these Guidelines. While carrying out their responsibilities under these Guidelines every member of a Regulated Entity's Senior Management shall exercise due skill, care and diligence.

CHAPTER-II

RISK-BASED APPROACH

2.1. (a) The primary thrust of these Guidelines is to enable a Regulated Entity to adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which the Regulated Entity is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same. A Regulated Entity while adopting RBA shall ensure that: -

(i) The RBA is objective and proportionate to the risks;

(ii) The RBA is based on reasonable grounds; and

(iii) The RBA is reviewed and updated at appropriate intervals.

(b) The RBA shall be appropriate to the nature and size of the business. While implementing the RBA, the Regulated Entity shall consider all relevant risk factors before deciding overall risk. Based on the risk assessment, the Regulated Entity shall monitor, manage, and mitigate the risks it is exposed to by applying effective, appropriate and proportionate measures.

(c) In addition to assessing the ML/TF risks presented by an individual customer, a Regulated Entity shall also identify and assess ML/TF risks at an enterprise-wide level [16][Financial Group-

[16] Inserted vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN)

wide level or Group-wide level], wherever applicable. This shall include a consolidated assessment of the Regulated Entity's ML/TF risks perception that exist across all its business units, product lines and delivery channels.

Explanation: FATF Public Statement, the reports and guidance notes on AML/CFT/PF issued by FATF and any country specific information that is circulated by relevant authorities from time to time, as well as the updated list of natural and legal persons who are subjected to sanction measures as required under various United Nations' Security Council Resolutions. etc., may also be used in risk assessment.

(d) The outcome of the risk assessment by a Regulated Entity shall be properly documented. The documentation should include the enterprise-wide AML/CFT risk assessment wherever applicable, details of the implementation of the AML/CFT risk management systems and controls as guided by the AML/CFT risk assessment. A Regulated Entity shall ensure that the ML/TF risk assessment information are made available to the Authority upon request. The records of documented risk assessment shall be kept as per the requirements of record keeping process specified under these Guidelines.

(e) The result of the risk assessment shall be used to classify the ML/TF risks as low, medium, and high. The general principle of this classification is to apply enhanced measures in case of high-risk customers and simplified measures in case of low-risk customers.

(f) To keep the risk assessments up-to-date, the Regulated Entity shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The outcome of the exercise shall be put up to the Governing Body or such other committee of the Regulated Entity to which power in this regard has been delegated.

Guidance Note: -

The RBA should be an essential foundation in Regulated Entity's AML-CFT compliance culture, and it must trickle down from the level of Senior Management to the rest of the organization.

CHAPTER- III

BUSINESS RISK ASSESSMENT

3.1. Identifying and Assessing business AML risks

A Regulated Entity shall:

(a) take into consideration the nature, size and the complexity of its business activities and take suitable steps to identify its exposure to ML/TF risks;

(b) consider the following risk factors, to the extent applicable and relevant, while identifying and assessing the ML/TF risks: -

(i) its type of customers and their activities.

(ii) its business engagement with the countries or geographic areas;

(iii) its products, services, delivery channels and activity profiles;

(iv) the complexity and volume of its transactions;

(v) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and

(vi) the use of new or developing technologies for both new and pre-existing products;

(c) based on the assessment and risk identification made at Clause (a) and (b) above, the Regulated Entity shall undertake commensurate mitigation measures.

3.2. New products, business practices and technologies

(a) A Regulated Entity shall identify and assess the ML and TF risks that may arise in relation to:-

(i) the development of new products, business practices, including new delivery mechanisms; and

(ii) the use of new or developing technologies for both new and pre-existing products.

(b) The Regulated Entity shall undertake the above risk assessment exercise, prior to the launch or use of such products, practices and technologies and shall take appropriate measures to manage and mitigate the risks.

Guidance Note: -

(1) One of the key reasons for undertaking the exercise of business risk assessment is that it will aid the Regulated Entity to better understand its exposure to ML/TF risks and then take appropriate measures to prevent its business being used for the purposes of ML/TF. The risk exposure of the Regulated Entity varies depending on several factors such as the nature of the business, the type of customers, the nature of the products, services offered and transactions and delivery channels involved.

(2) The outcome of the business risk assessment should be used by a Regulated Entity to gauge its own vulnerabilities to ML/TF risks and to take all necessary measures to mitigate such risks.

(3) The outcome of the business risk assessment shall be factored into while assessing the customer risk assessment, in the manner as specified under Chapter IV.

3.3. AML/CFT systems and controls

(a) The nature and extent of AML/CFT systems and controls implemented by a Regulated Entity shall be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk

assessment, wherever applicable. A Regulated Entity shall put in place adequate policies, procedures, systems and controls to mitigate such ML/TF risks. The information obtained from the risk assessment shall be used to:

(i) establish and maintain effective policies, procedures, systems and controls to prevent ML/TF;

(ii) ensure that Regulated Entity's AML/CFT policies, procedures, systems and controls adequately mitigate the risks identified under Clause 3.1 above;

(iii) ensure that Regulated Entity's systems and controls:

(aa) include a provision enabling its Senior Management to regularly review the information on operations and effectiveness of its AML systems and controls;

(bb) enable the Regulated Entity to determine:

(1) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP); and

(2) whether a beneficiary of the policy, or a Beneficial Owner of such beneficiary is a PEP, (in the cases where it is providing life insurance or other similar policies); and

(3) enable a Regulated Entity to comply with these Guidelines and applicable AML-CFT legislations.

(iv) ensure that regular risk assessments are carried out on the adequacy of the Regulated Entity's AML/CFT systems and controls to enable it to identify, assess, monitor, manage and mitigate such risks adequately.

(b) The AML/CFT policies, procedures and controls shall be approved by Senior Management to enable a Regulated Entity to effectively manage and mitigate the risks either identified by it or notified to it by the Authority or other relevant authorities. Further, the Regulated Entity shall constantly monitor the implementation of the policies, procedures and controls, and improve them, if necessary.

Guidance Note

(1) A Regulated Entity's ML/TF risk assessment serves as a guide to the allocation of AML/CFT resources within it.

(2) In the context of Clause (a) (iii) (bb) (2) above, a beneficiary may be a natural person, legal person, legal arrangement, or category of persons who will be paid the policy proceeds when an insured event occurs, that is covered by the policy.

CHAPTER-IV

CUSTOMER RISK ASSESSMENT

Risks identified while assessing the business risks shall be used for the customer risk assessment. The customer risk assessment shall be performed while taking into consideration the parameters, or

the process as specified below. The outcome of the Customer risk assessment shall be used to assign the risk rating of the customer as high, medium or low, proportionate to the ML/TF risks.

4.1. Assessing customer AML risks

(a) A Regulated Entity shall:

(i) undertake a risk-based assessment of every customer; and

(ii) assign the customer a risk rating proportionate to the ML/TF risks.

(b) The customer risk assessment referred to in Clause (a) above, shall be completed prior to undertaking Customer Due Diligence for new customers, and also where the Regulated Entity otherwise feels necessary, for existing customers.

(c) When undertaking an assessment under Clause 4.1 (a) (i) above, a Regulated Entity shall:

(i) identify the customer and Beneficial Owner, if any;

(ii) obtain information on the purpose and intended nature of the business relationship;

(iii) obtain information on, and take into consideration, the nature of the customer's business;

(iv) take into consideration the nature of the customer, its ownership, control structure, and its Beneficial Ownership, wherever applicable;

(v) take into consideration the nature of the customer's business relationship with the Regulated Entity;

(vi) take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;

(vii) take into consideration the relevant product, service or transaction; and,

(viii) take into consideration the beneficiary of the policy including any Beneficial Owner of such beneficiary, if it is providing the customer with a life insurance or other similar policy.

[17][(d) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off.]

4.2. Factors that may indicate high ML/TF risk

When assessing if there is a high risk of ML/TF in a particular situation, a Regulated Entity shall take into account, among other things:

(a) Customer risk

(i) Whether the customers are from high risk businesses / activities / sectors, as well as from other sectors as may be identified by it;

[17] Inserted vide Circular dated January 02, 2026

(ii) Whether the ownership structure of the legal person or arrangement appears unusual or excessively complex;

(iii) Whether the business relations are conducted under unusual circumstances (e.g., significant unexplained geographic distance between the Regulated Entity and the customer);

(iv) Whether the companies have nominee shareholders or shares in bearer form;

(v) Whether the legal persons or legal arrangements are personal asset holding vehicles; and,

(vi) Whether the corporate structure of the customer is unusual or excessively complex given the nature of the business.

(b) <u>Country or Geographic risk</u>

(i) Whether the countries or jurisdictions the Regulated Entity is exposed to, either through its own activities (including where its branches and subsidiaries operate in) or the activities of its customers (including the Regulated Entity's network of correspondent account relationships) have relatively high levels of corruption, organized crime or inadequate AML/CFT measures, as identified by the FATF;

(ii) Whether the countries or jurisdictions are identified by any credible body as having significant levels of corruption, terrorism financing or other criminal activities;

(iii) Whether the countries or jurisdictions are identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;

(iv) Whether the countries or jurisdictions do not have effective systems to counter ML/TF; or not implementing the AML/CFT measures that are consistent with FATF recommendations;

(v) Whether the countries or jurisdictions are subject to sanctions, embargos or similar measures issued by International Organisations or India;

(vi) Whether the countries or jurisdictions are funding or supporting the terrorism; and,

(vii) Whether countries or jurisdictions have organizations operating within their territory that have been designated by India, other countries or International Organizations as terrorist organizations.

(c) <u>product, service, transaction or delivery channel risk factors</u>

(i) Whether the service involves private banking;

(ii) Whether the product, service or transaction is one that might favour anonymity;

(iii) Whether the situation involves non-face-to-face business relationships or transactions, without adequate safeguards;

(iv) Whether the payments received are from unknown or unassociated third parties;

(v) Whether the services offered are in relation to nominee directors, nominee shareholders or the formation of companies in another country; and

(vi) Whether there are anonymous transactions or any transaction which involves frequent payments, received from unknown or unassociated third parties.

When assessing the risk factors, the Regulated Entity shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a high risk of ML/TF in a particular situation.

4.3. Factors that may indicate low ML/TF risks

When assessing if there is a low risk of ML/TF in a particular situation, a Regulated Entity shall take into account, among other things:

(a) Customer risk factors, including whether the customer is:

(i) a Government entity;

(ii) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.

(iii) regulated financial institution incorporated or established outside India that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

(iv) a subsidiary of a regulated financial institution referred to in sub-clause (iii) above, if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML standards as that of its Parent entity;

(v) a public body or a publicly owned enterprise;

(vi) a resident established or registered in a geographical area of low risk;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(i) a Contract of Insurance that is non-life insurance;

(ii) a Contract of Insurance that is a life insurance product with no investment return or redemption or surrender value;

(iii) an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;

(iv) a Contract of Insurance which is a reinsurance contract that is ceded by an insurer which is a regulated financial institution;

(v) a pension, superannuation or similar scheme that satisfies the following conditions:

(aa) the scheme provides retirement benefits to employees;

(bb) contributions to the scheme are made by way of deductions from wages; and

(cc) the scheme rules do not permit the assignment of a member's interest.

(vi) a product where the ML/TF risks are adequately managed by other factors such as transaction limits or transparency of ownership; and

(vii) financial products or services that provide appropriately defined and limited services to certain types of customers (e.g., to increase customer access for financial inclusion purposes).

When assessing the risk factors, the Regulated Entity shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a low risk of ML/TF in a particular situation.

4.4. Business relationship should not be established in the following cases:

The Regulated Entity shall not establish the business relationship with the customer, which is a legal person or legal arrangement, in the following cases: -

(a) where the ownership or control arrangements of the customer prevent the Regulated Entity from identifying one or more of the customer's Beneficial Owners;

(b) where there are anonymous accounts, Acccounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the Regulated Entity; or

(c) a Shell Financial Institution.

Guidance Note for customer risk assessment

(1) The risk assessment requires a Regulated Entity to allocate an appropriate risk rating to every customer. The risk ratings should be descriptive, such as "low", "medium" or "high". The outcome of the ML/TF risk assessment decides the degree of Customer Due Diligence that need to be performed. For a high-risk customer, the Regulated Entity shall undertake Enhanced CDD measures in addition to the normal CDD. For a low-risk customer, the Regulated Entity may undertake Simplified CDD. For any other customer, the Regulated Entity may undertake the normal CDD.

(2) Where information obtained as part of CDD alters the risk rating of a customer, such change should reflect in its CDD being undertaken.

CHAPTER- V

CUSTOMER DUE DILIGENCE

5.1. A Regulated Entity after assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the Customer Due Diligence. While undertaking the CDD, a Regulated Entity shall: -

(i) undertake Customer Due Diligence measures as detailed under Clause 5.4, in respect of all the customers;

(ii) undertake Enhanced Customer Due Diligence measures as detailed under Clause 5.6, in addition to the CDD measures detailed under Clause 5.4, in respect of the customer who has been assigned 'high risk'; and,

(iii) undertake Simplified Customer Due Diligence measures as detailed under Clause 5.7 by modifying Customer Due Diligence process detailed under Clause 5.4, in respect of a customer who has been assigned 'low risk'.

5.2. Timing of CDD

(a) Except as otherwise provided in Clause 5.3 and 5.4, a Regulated Entity shall undertake the Customer Due Diligence of a customer: -

(i) at the time of establishing business relationship, as mandated under Clause 5.4.1 (a) to (c); and,

(ii) after establishing a business relationship, as mandated under Clause 5.4.1.(d).

(b) A Regulated Entity shall also undertake Customer Due Diligence if, at any time:

(i) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;

(ii) it suspects ML/TF; or,

(iii) there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

5.3. Establishing business relationship before verification

(a) A Regulated Entity may establish a business relationship with a customer before completing the verification required under Clause 5.4.1, subject to fulfilling the following conditions:

(i) the deferral of completion of the verification of the customer or Beneficial Owner is essential in order not to interrupt the normal conduct of a business relationship;

(ii) there is low risk of occurrence of ML/TF activity and any such risks identified can be effectively managed by the Regulated Entity;

(iii) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed, and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and

(iv) subject to Clause 5.3 (b) below, the relevant verification is completed as soon as reasonably practicable and, in any event, it should not exceed 30 business days after the establishment of business relationship.

(b) Where a Regulated Entity is not able to comply with the 30-day requirement, it shall, prior to the end of the 30-day period:

(i) document the reason for its non-compliance;

(ii) complete the verification as soon as possible; and

(iii) record the non-compliance event for reporting to its Governing Body.

(c) The Regulated Entity shall suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that is possible) if such verification remains uncompleted for 30 days after the establishment of business relationship.

(d) The Regulated Entity shall terminate business relations with the customer if such verification remains uncompleted for 120 days after the establishment of business relationship.

(e) A Regulated Entity shall ensure that its AML/CFT systems and controls referred to in Clause 3.3 above, include internal risk management policies and procedures concerning the conditions under which such business relationships may be established with a customer before completing verification and should also factor the above time limitation in its policies, procedures and controls.

Guidance Note: -

(1) Examples of the situations which might lead a Regulated Entity to have doubts about the veracity or adequacy of documents, data or information previously obtained, could be where there is a suspicion of ML/TF in relation to that customer, or where there is a material change in the manner the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Regulated Entity that a person other than the customer is the real customer.

(2) Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, may include:

(i) Non-face-to-face business.

(ii) Securities transactions.

In the securities market, companies and intermediaries may be required to perform transactions without delay depending upon market conditions, and in such circumstances, the execution of the transaction may be required before verification of identity is completed. Similar circumstances may occur where the customer seeks immediate insurance cover.

(3) In case the Regulated Entity is not able to complete customer due diligence as required under Clause 5.4, it shall not commence or continue business relations with any customer or undertake any transaction for any customer. In case of failure to complete customer due diligence in the prescribed time limit, the Regulated Entity shall apply appropriate measures as specified under Clause 5.10. A Regulated Entity shall also consider filing of STR if the circumstances are suspicious.

(4) A Regulated Entity shall also adopt risk management procedures in the cases specified under Clause 5.3. These procedures shall include a set of measures, such as a limitation of the number, types and/or value of transactions that can be performed. The procedures shall also include the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. In such situations, a Regulated Entity shall ensure close monitoring, until the verification is completed.

5.4. Customer Due Diligence Requirements

5.4.1. Undertaking Customer Due Diligence (CDD)

In undertaking Customer Due Diligence as required under Clause 5.1.(a) (i), the following measures shall be undertaken by a Regulated Entity: -

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that the Regulated Entity is satisfied that it knows who the beneficial owner is. Similarly, for legal persons and arrangements, the CDD shall include Regulated Entity taking reasonable steps to understand the nature of the customer's business, its ownership and control structure.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Regulated Entity's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

5.4.2. Identification of Customer

(a) If a customer is a natural person, a Regulated Entity shall obtain at least the following information:
   (i) Full name, including any aliases;
   (ii) Unique Identification Number (such as an Identity card number, passport number, etc.);
   (iii) Date of birth;
   (iv) Nationality;
   (v) Legal domicile;
   (vi) Current residential address; (other than a post office box address);
   (vii) Contact details such as personal, office or work telephone numbers.

(b) If a customer is a legal person or legal arrangement, a Regulated Entity shall obtain at least the following information:
   (i) The full name and any trading name;
   (ii) Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);
   (iii) Registered or business address, and if different, its principal place of business;
   (iv) Date of establishment, incorporation or registration;
   (v) Place of incorporation or registration.

(c) Further, in cases where the customer is a legal person or legal arrangement, a Regulated Entity shall, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. In addition to this, Regulated Entity shall also identify and screen the related parties or connected parties of such customer and should remain appraised of any changes to connected parties. For identification of the connected parties, a Regulated Entity shall obtain at least the following information of each related or connected party:
   (i) full name, including any aliases; and
   (ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

Guidance Note: -

(1) The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties, or which is his place of origin.

(2) A Regulated Entity should exercise greater caution when dealing with an unfamiliar or a new customer. Apart from obtaining the identification information required under Clause 5.4.2 (a),

a Regulated Entity should (if not already obtained as part of its account opening process) also obtain additional information on the customer's background such as occupation, employer's name, nature of business, range of annual income, other related accounts with the same Regulated Entity and whether the customer holds or has held a prominent public position. Such additional identification information enables a Regulated Entity to obtain better knowledge of its customer's risk profile, as well as the purpose and intended nature of the account.

(3) Identification of connected parties or related parties may be undertaken using publicly available sources or databases such as company registries, annual reports. Additionally, it could be based on substantiated information provided by the customers.

5.4.3. <u>Verification of Identity of Customer</u>

(a) A Regulated Entity shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, a Regulated Entity shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.

(b) When relying on documents, a Regulated Entity should be aware that the most reliable documents to verify the identity of the customer are those which are most difficult to obtain illegally or to counterfeit. These may include government-issued identity cards or current valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process should be commensurate with the customer's risk profile.

(c) In verifying the identity of a customer, a Regulated Entity may obtain the following documents:

<u>In case of Natural Persons –</u>

(i) any of the OVD specified under these Guidelines that contains photograph of the customer, name, unique identification number, date of birth and nationality; and

(ii) residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

<u>In case of Legal persons or Legal Arrangements-</u>

(i) **<u>Name, legal form, proof of existence and constitution:</u>** - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and

(ii) **<u>Powers that regulate and bind the legal person or legal arrangement</u>**:- This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement

and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories.

Guidance Note: -

(1) In cases where a customer is a natural person, the Regulated Entity shall obtain the OVD that contain a clear photograph of that customer.

(2) In cases where a customer is a foreign national, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national would also be considered as OVD. In case where the customer is an Indian national, OVD shall include the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card, etc. as prescribed under the Rules (For more detailed understanding, refer OVD definition). For the purpose of customer verification, equivalent e-documents of OVDs shall also be treated as original document by a Regulated Entity.

(3) [18][Where a customer submits any documents other than Post Office savings bank account statement or statement of a bank account including of a foreign bank, as specified at the third proviso of clause 1.3.30 for limited purpose of proof of address, such customer shall submit updated OVD or their equivalent e-documents thereof with current address within a period of three months of submitting the documents specified at the third proviso of clause 1.3.30 above.

Explanation: The bank account or Post Office savings bank account statement or statement of foreign bank may be accepted as deemed OVD for the limited purpose of proof of address, only for such customers where simplified measures are applied.]

(4) While undertaking CDD for different customers (including legal persons or legal arrangements), a Regulated Entity should obtain such information and documents as required under these Guidelines. Illustrative list of information and documents which should be obtained for onboarding customers are specified in Annexure I of these Guidelines.

---

[18] Substituted for "In cases where other than simplified measures are applied, the customer shall submit updated OVD or their equivalent e-documents thereof with current address within a period of three months of submitting the documents specified at the third proviso of Clause 1.3.30 above."

Explanation: - For those customers to whom simplified measures are not applied, the bank account or Post Office savings bank account statement or statement of foreign bank shall not be accepted as deemed OVD for the limited purpose of proof of address." vide Circular dated June 05, 2025 (the Circular can be accessed at https://shorturl.at/4BrTr).

(5) Further, for onboarding Indian Nationals, a Regulated Entity may follow the procedure as specified under Annexure-2 of these Guidelines.

(6) A Regulated Entity should examine the original identification documents and retain a copy of the same. However, in complying with Clause 5.4.1, (i.e., undertaking customer due diligence), at times, if a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where Regulated Entity has no physical contact with the customer or the onboarding of customer is done through non-face to face mode), a Regulated Entity should obtain a copy of the document that is certified to be a 'true copy' and such certification may be carried out by person specified in Clause 1.3.7 of these Guidelines.

(7) The Regulated Entity shall ensure that documents obtained for performing CDD, as required under these Guidelines, are clear and legible. This is important for the establishment of a customer's identity, particularly in situations where business relations are established through non-face to face mode.

(8) Except for high-risk customers, the following mode of verifications are also considered as sufficient to satisfy the requirements of Clause 5.4.3: -

(i) downloading publicly available information from an official source (such as a regulator's or other official government website);

(ii) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases, provided that the commercial database is recognized for such purpose by the home regulator, if any, of the database.

(9) Where a Regulated Entity obtains data, documents or information from the customer or a third party, it shall ensure that such data, documents or information is up-to-date.

(10) Where the customer is rated as high-risk, the identification information shall be independently verified, using both public and non-public sources.

5.4.4. <u>Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer</u>

(a) Where a customer is a natural person or legal person [19][or legal arrangement], to act on its behalf for establishing business relations with a Regulated Entity, the Regulated Entity shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person [20][or legal arrangement] by obtaining information as specified in Clause 5.4.2 above.

[19] Inserted vide Circular dated January 02, 2026.
[20] Inserted vide Circular dated January 02, 2026.

[21][*Provided that* in case of a trust, the Regulated Entity shall ensure that trustees disclose their status at the time of commencement of a business relationship or when carrying out transactions as specified in clause (b) of sub-rule (1) rule 9 of the Rules].

(b) Further, the Regulated Entity shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, the Regulated Entity shall verify the authorization of each natural person appointed to act on behalf of the customer by obtaining at least the following:

(i) The appropriate documentary evidence authorizing the appointment of such natural person by the customer to act on his or its behalf which may include power of attorney, resolution passed by Governing Body or authorization granted to transact on its behalf.

(ii) Where there is a long list of natural persons appointed to act on behalf of the customer (e.g., a list comprising more than 10 authorized signatories), the Regulated Entity shall verify those natural persons who will deal directly with the Regulated Entity.

5.4.5. Identification and Verification of Identity of Beneficial Owners

Where there is one or more Beneficial Owners in relation to a customer, the Regulated Entity shall identify the Beneficial Owners and take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources.

For the identification and verification of Identity of Beneficial Owner, the Regulated Entity should consider the following in relation to:

(a) Customers that are legal persons

(i) The identity of the natural person(s) (whether acting alone or together) exercising control over the legal person through ownership or who ultimately owns the legal person;

(ii) To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural person(s) (if any) who ultimately control the legal person or have ultimate effective control over the legal person.

(b) Customers that are legal arrangements

(i) 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 [22][ten] per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

[21] Inserted vide Circular dated September 8, 2023 (the Circular can be accessed at https://shorturl.at/MwsLx).
[22] Substituted for "fifteen" vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).

(ii) In all other types of legal arrangements, the Regulated Entity shall identify persons in equivalent or similar positions.

5.4.6. Parameters to Identify and Verify the Identity of Beneficial Owners: -

(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 or entitlement to more than [23][ten] 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 [24][ten] per cent. of capital or profits of the partnership [25][or who exercises control through other means.

Explanation - For the purpose of this clause, "Control" shall include the right to control the management or policy decision;];

(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 or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (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 fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

---

[23] Substituted for "twenty-five" vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).

[24] Substituted for "fifteen" vide Circular dated September 8, 2023 (the Circular can be accessed at https://shorturl.at/MwsLx).

[25] Inserted vide Circular dated September 8, 2023 (the Circular can be accessed at https://shorturl.at/MwsLx).

5.4.7. As per rule 9(3)(f) of the Rules, unless the Regulated Entity has doubts about the veracity of the CDD information, or suspects that customer may be connected with ML/TF, it shall not be required to identify and verify the identity of any shareholder or beneficial owner of a customer in the following -

Where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a customer under the Act and Rules.

5.4.8. As per the [26][second proviso of rule 9(1)(c)] of the Rules, in cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in sub-rules (3) to (9) of the rule 9 of the Rules shall be applicable for due-diligence of such beneficial owner.

Guidance Note: -

(1) For opening an account of a Legal Person who is not a natural person, the Regulated Entity has to identify the beneficial owner(s) and shall undertake all reasonable steps to verify his/her identity in terms of sub- rule (3) of rule 9 of the Rules.

(2) A Regulated Entity may also consider obtaining an undertaking or declaration from the customer on the identity of, and the information relating to, the beneficial owner.

(3) Notwithstanding the obtaining of such an undertaking or declaration, the Regulated Entity remains responsible for complying with the obligations under the Guidelines to take reasonable measures to verify the identity of the beneficial owner by, for example, researching publicly available information on the beneficial owner or arranging a face-to-face meeting with the beneficial owner, to corroborate the undertaking or declaration provided by the customer.

(4) Where the customer is not a natural person and has a complex ownership or control structure, a Regulated Entity should obtain enough information to sufficiently understand if there are legitimate reasons for such ownership or control structure.

(5) Where the Regulated Entity has exhausted all possible means but has not been able to identify the Beneficial Owners under Clause 5.4.5., it shall treat the Senior Management of the said legal person or legal arrangement, as the Beneficial Owners. However, in such cases, the

[26] Substituted for 'proviso of rule 9(1)(b)' vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

Regulated Entity shall keep a record of all the actions it has taken to identify the Beneficial Owners of such legal persons or legal arrangement.

(6) If the ownership or control arrangements of a customer are of such a nature that the Regulated Entity is prevented from identifying the Beneficial Owners, the Regulated Entity shall not establish a business relationship with the customer under Clause (a) of 4.4.

(7) In relation to Clause 5.4.7 and Clause 5.4.8 above, currently the notified jurisdictions by Central Government are as follows: -

(i) United States of America

(ii) Japan

(iii) South Korea

(iv) United Kingdom excluding British Overseas Territories

(v) France

(vi) Germany

(vii) Canada

(8) Where the customer is not a natural person, the Regulated Entity shall understand the nature of the customer's business, its ownership and control structure, before opening an account.

5.4.9. <u>Identifying and verifying beneficiary of a life insurance policy</u>

(a) For life or other investment-related insurance business, Regulated Entity shall, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(i) A Regulated Entity shall, as soon as a beneficiary of a life policy is identified as a specifically named natural person, legal person or legal arrangement, obtain the full name, including any aliases, of such beneficiary;

(ii) For beneficiary(ies) that are designated by characteristics or by class (e.g., spouse or children at the time that the insured event occurs) or by other means (e.g., under a will) – the Regulated Entity shall obtain sufficient information concerning the beneficiary(ies) to satisfy itself that it will be able to establish the identity of the beneficiary(ies) at the time of the payout.

[27][(iii) In relation to life insurance policies, the Regulated Entity should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to

[27] Inserted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/yuyn1).

inform Senior Management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a Suspicious Transaction Report.]

Guidance Note: -

(1) For both the cases referred to in (i) and (ii) of the Clause 5.4.9 (a) above, the verification of the identity of the beneficiary(ies) should be conducted at the time of the payout.

(2) The information collected under (i) and (ii) of the Clause 5.4.9 (a) above, should be recorded and maintained in accordance with the record keeping requirements under these Guidelines.

(3) The beneficiary of a life insurance policy should be included as a relevant risk factor by the Regulated Entity in determining whether enhanced CDD measures are applicable. If the Regulated Entity determines that a beneficiary who is a legal person or a legal arrangement presents a high risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

5.4.10. Information on the Purpose and Intended Nature of Business Relations

(a) A Regulated Entity shall, while establishing business relationships, understand and as appropriate, obtain information from the customer as to the purpose and intended nature of business relations.

(b) The measures taken by a Regulated Entity to understand the purpose and intended nature of business relations should be commensurate with the risk profile and complexity of the customer's business.

5.5. Accounts of Politically Exposed Persons

(a) A Regulated Entity shall implement appropriate internal risk management systems, policies and procedures to determine if a customer or any natural person appointed to act on behalf of the customer, or any beneficial owner of the customer is a politically exposed person (PEP) or in case of a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP.

(b) A Regulated Entity shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer or beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary is determined by the Regulated Entity to be a PEP:

(i) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives;

(ii) Verify the identity before accepting the PEP as a customer;

(iii) Obtain approval from its Senior Management before opening an account of a PEP or making any payout under the life insurance or other similar policy to the PEP;

(iv) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;

(v) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

(vi) Carry out the additional Customer Due Diligence for circumstances specified in sub-clauses (i) to (v) above, before making any payout under the life insurance or other similar policy.

(c) A Regulated Entity may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for:-

(i) PEP, their family members and close associates;

(ii) International Organisation PEP, their family members, and close associates; or

(iii) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Regulated Entity present a high risk for ML/TF.

Guidance Note: -

(1) A Regulated Entity is required to take reasonable measures to determine whether a customer or beneficial owner is a PEP or a person who is or has been entrusted with a prominent function by an international organisation.

(2) A Regulated Entity shall also ascertain the source of wealth of the customers by appropriate and reasonable means. (Examples of appropriate and reasonable means of establishing source of wealth are information and documents such as evidence of title, copies of trust deeds, audited accounts, salary details, tax returns, bank statements, etc.).

(3) A Regulated Entity should be aware that customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves. Therefore, the measures applied for all types of PEPs should also apply to family members or close associates of such PEPs.

(4) A Regulated Entity should not automatically treat all individuals who are PEPs, as a high-risk customer. Each PEP should be assessed on risk sensitive basis and the Regulated Entity shall determine what risk category is appropriate for such PEPs. In case a PEP is assigned as high risk, the Regulated Entity shall undertake the Enhanced Customer Due Diligence measures referred under Clause 5.6. However, even if a PEP is not assigned a high risk, the Regulated

Entity shall still undertake the additional customer due diligence measures specified in Clause 5.5 (b) for PEPs.

(5) Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth (i.e., total assets). This relates to how the customer and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information should give an indication about the size of wealth the customer and beneficial owner would be expected to have. Although the Regulated Entity may not have specific information about assets that are not deposited with or processed by the Regulated Entity, it may be possible to obtain general information from the customer, commercial databases or other open sources.

(6) Verification of source of wealth can be carried out by various measures including obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, information and documents such as evidence of title, copies of trust deeds, bank or brokerage account statements, probate documents, audited accounts and financial statements, salary details, tax returns, news items from a reputable source and other similar evidence. For instance:

(i) for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and

(ii) for a natural person, this might include documentary evidence which corroborates answers given to questions on the source of wealth in an application form or customer questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide bank statements, salary statements or tax returns covering number of years to draw up a picture of his source of wealth.

5.6. Enhanced Due Diligence

(a) Where the risks of ML/TF are high, a Regulated Entity shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows: -

(i) Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner.

(ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.

(iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

(iv) Obtaining the approval of Senior Management to commence or continue the business relationship.

(v) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,

(vi) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

(b) Where applicable, it is required that first payment made by a customer in order to open an account with a Regulated Entity shall be carried out through a bank account in the customer's name with:

(i) a Bank;

(ii) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or

(iii) a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

(c) [28][The Regulated Entities shall specifically apply enhanced due diligence measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.]

Guidance Note: -

(1) The Enhanced CDD measures will apply depending upon the risk profile of the customer and the extent of its applicability to a customer shall be decided on case-to-case basis.

(2) Circumstances where a customer presents or may present a high probability of ML/TF risk may include, but are not limited to the following:

(i) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; and

[28] Inserted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).

(ii) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the Regulated Entity for itself or notified to Regulated Entity generally by the Authority or other relevant domestic authorities in India or other foreign regulatory authorities.

(3) For establishing an account-based relationship with high-risk customers, the approval may be given by Senior Management or committee of senior managers or an individual member who has been authorised by the Senior Management in this behalf.

(4) In cases where a customer uses complex legal structures and/or trusts, private investment vehicle, the Regulated Entity shall satisfy itself that it is used for a legitimate and genuine purpose.

(5) The Regulated Entity shall take reasonable measures to examine the source of wealth and source of funds. That is, where the funds for a particular service or transaction will come from (e.g., a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.

(6) Source of funds refers to the origin of the particular funds or other assets which are the subject of the establishment of business relations. In order to ensure that the funds are not proceeds of crime, the Regulated Entity should not limit its source of funds inquiry to identifying the other financial institution from which the funds have been transferred, but more importantly, the activity that generated the funds. The information obtained should be substantive and facilitate the establishment of the provenance of the funds or reason for the funds having been acquired.

(7) Examples of appropriate and reasonable means of establishing source of funds are such as proof of dividend payments connected to a shareholding, bank statements, salary payments or bonus certificates, sale proceeds, loan documentation and proof of a transaction which gave rise to the payment into the account.

(8) A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

[29][(9) To maintain transparency and mitigate the risk of round-tripping, the Regulated Entity shall endeavor to ascertain the source of funds in cases where the Beneficial Owner of an entity is an Indian National. In such instances, the Regulated Entity shall apply the enhanced

[29] Inserted vide Circular dated January 02, 2026.

due diligence measures specified under point (ii) of sub-clause (a) of clause 5.6 above, irrespective of the risk categorization assigned to such Non-Resident customer.]

5.7. Simplified Customer Due Diligence

(a) Where the risks of ML/TF are low, a Regulated Entity may conduct simplified CDD measures, which should be commensurate with the low risk factors. Examples of possible measures are:

(i) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship as specified under Clause 5.3.

(ii) Reducing the frequency of customer identification updates.

(iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

(iv) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

(b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.

Guidance Note: -

(1) Where a Regulated Entity applies SCDD measures, it is still required to perform ongoing monitoring of business relations as specified under Clause 5.8.

(2) A Regulated Entity is not required to identify or verify Beneficial Owners for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions.

(3) The Regulated Entity may also use other measures to conduct CDD in accordance with the customer risks.

5.8. Ongoing customer due diligence

While undertaking the ongoing customer due diligence, as required under Clause 5.4.1.(d), the following requirements shall be complied with by a Regulated Entity: -

(i) The Regulated Entity shall monitor its business relations with the customer on an ongoing basis.

(ii) The Regulated Entity during the course of business relations with a customer, shall observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with Regulated Entity's knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.

(iii) The Regulated Entity shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.

(iv) The Regulated Entity shall make further enquiries into the background and purpose of the transaction specified in sub-clause (iii) above, and document its findings so that this information is made available to the relevant authorities, should the need arise.

(v) A Regulated Entity shall periodically review each customer to ensure that the risk rating assigned under Clause 4.1. (a) (ii) above, is commensurate with the ML/TF risks posed by the customer.

(vi) Where there are indications that the risks associated with an existing business relation with the customer may have increased, the Regulated Entity shall request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

(vii) The Regulated Entity shall ensure that the Customer Due Diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Customer Due Diligence data, documents and information, particularly for customers with high-risk rating.

Guidance Note: -

(1) For an effective and robust AML/CFT risk management system, a Regulated Entity shall follow the process of Ongoing monitoring of all business relations. However, the rigor and extent of monitoring of a customer shall be determined based on the customer's ML/TF risk profile.

(2) An essential aspect of ongoing monitoring includes maintaining up-to-date and relevant Customer Due Diligence data, documents and information so that the Regulated Entity can identify the changes in customer's risk profile. The following shall be followed by the Regulated Entity: -

(i) for customers who are rated as high risk, the Regulated Entity shall obtain updated CDD information (including updated copies of the customer's Officially Valid Documents if these have expired), as part of its periodic CDD review, or upon the occurrence of a trigger event as deemed necessary by the Regulated Entity, whichever is earlier; and

(ii) for all other risk categories of customers, a Regulated Entity should obtain updated CDD information upon the occurrence of a trigger event.

(3) A Regulated Entity shall undertake a review under sub-clause (v) and (vii) of Clause 5.8, both periodically and at other appropriate times, including when:

(i) the Regulated Entity changes its CDD documentation requirements;

(ii) an unusual transaction with the customer is expected to take place;

(iii) there is a material change in the business relationship with the customer; or

(iv) there is a material change in the nature or ownership of the customer.

5.9. Ongoing sanctions screening

A Regulated Entity shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list when complying with Clause 5.4.1 (d).

5.10. Failure of Regulated Entity to conduct or complete customer due diligence

(a) In cases where a Regulated Entity is unable to conduct or complete the requisite Customer Due Diligence for a customer in accordance with Clause 5.4.1, it, to the extent relevant, shall: -

(i) not open an account or otherwise provide a service;

(ii) not carry out a transaction with or for the customer;

(iii) not otherwise establish a business relationship;

(iv) terminate or suspend any existing business relationship with the customer;

(v) return any monies or assets received from the customer; and,

(vi) consider whether the failure to conduct or complete Customer Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).

[30][Provided that no application for onboarding or periodic updation of KYC shall be rejected, in case of Persons with Disabilities (PwDs), without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.]

(b) A Regulated Entity is not bound to comply with sub-clauses (a) (i) to (v) above, if it amounts to "tipping off" of the customer, or FIU-IND directs the Regulated Entity to act otherwise.

Guidance Note: -

(1) A Regulated Entity while complying under Clause 5.10 (a), should apply one or more of the measures specified under sub-clauses (i) to (vi) above, as applicable, in the circumstances. In cases where CDD cannot be completed, it is appropriate that the Regulated Entity shall not carry out transaction until the completion of pending CDD.

[30] Inserted vide Circular dated January 02, 2026.

(2) Clause 5.10 shall apply to both existing and prospective customers. In case of existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances.

(3) The Risk Based Approach shall be adopted for the Customer Due Diligence of the existing customers.

5.11. Periodic Updation

A Regulated Entity shall adopt a risk-based approach for periodic updation of CDD. The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows: -

(i) Annually- for high-risk customers;

(ii) once in three years- for medium risk customer; and,

(iii) once in every five years- for low-risk customers.

[31][*Provided that* the periodicity of such updation in case of resident Indian customer having an existing client relationship with the Financial Group in India, shall be as follows:

(a) once in every two years - for high-risk customers,

(b) once in every eight years - for medium risk customers and

(c) once in every ten years - for low-risk customers.

Provided further that where the risk categorization made by the Financial Group entity differs from the risk categorization made by the Regulated Entity, the stricter of the two periodicity shall apply.]

[32]**[*Explanation.-*** Policy in this regard shall be documented as part of Regulated Entity's internal KYC policy, which is duly approved by the Governing Body of the Regulated Entity.]

(a) Individual Customers:

(i) No change in CDD information:

In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Regulated Entity or through digital channels (such as online banking / internet banking, e-mail or mobile application of Regulated Entity).

(ii) Change in address:

(aa) In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customer through customer's email-id registered with the Regulated Entity, customer's mobile number registered with the Regulated

[31] Inserted vide Circular dated January 02, 2026.
[32] Substituted vide Circular dated January 02, 2026.

Entity, digital channels (such as online banking internet banking, e-mail or mobile application of the Regulated Entity). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

(bb) Further, a Regulated Entity shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the Regulated Entity in its internal KYC policy, duly approved by its Governing Body.

(b) Customers other than Natural Persons:

(i) No change in CDD information:

In case of no change in the CDD information of a customer, which is a non-natural person, a self-declaration through email id registered with the Regulated Entity, digital channels (such as online banking / internet banking, mobile application of Regulated Entity), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the customer. Further, a Regulated Entity shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.

(ii) Change in CDD information:

In case of change in CDD information, Regulated Entity shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

(c) Additional measures:

In addition to the above, a Regulated Entity shall ensure that:

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

(ii) In case of Indian National, the customer's PAN details, if available with the Regulated Entity, is verified from the database of the issuing authority at the time of periodic updation of CDD.

(iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the Regulated Entity shall ensure that the information / documents obtained from the customers at the time of periodic updation of CDD are promptly updated

in its records / database and an intimation, mentioning the date of updation of CDD details, is provided to the customer.

(iv) In order to ensure customer convenience, a Regulated Entity may consider making available the facility of periodic updation of CDD at any of its branch, or in such other facilities in terms of its internal KYC policy, duly approved by its Governing Body.

(v) A Regulated Entity shall adopt a risk-based approach with respect to periodic updation of CDD. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Regulated Entity (such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of CDD only where account is maintained, a more frequent periodicity of CDD updation than the minimum specified periodicity etc.), shall be clearly specified in its approved internal KYC policy.

(vi) A Regulated Entity shall ensure that its internal KYC policy and processes on updation / periodic updation of CDD are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

[33][(vii) In case of any update in the documents submitted by the customer at the time of establishment of business relationship and thereafter, as necessary; customers shall submit to the Regulated Entity the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Regulated Entity's end.]

CHAPTER-VI

THIRD PARTY RELIANCE

6.1. For the purposes of these Guidelines, "Third Party" shall mean-

(a) A financial institution which is subject to and supervised by a financial regulator; or

(b) In relation to a Regulated Entity, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations;

AND

(c) Has an existing client relationship with a person whose data would be used for CDD and customer verification by a Regulated Entity.

6.2. A Regulated Entity may rely on a Third Party to perform CDD measures, subject to the following conditions:

(a) The Regulated Entity shall obtain records or information of the client due diligence carried out by the third party, [34][immediately];

[33] Clarified vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).
[34] Substituted for "within 2 days" vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

(b) The Regulated Entity shall take adequate steps to satisfy itself that the copies of identification data and other relevant documentation relating to the client due diligence will be made available by the third party upon request, without delay;

(c) The Regulated Entity is satisfied that the third party, it intends to rely upon, is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements mentioned under recommendation 10 and 11 of the FATF recommendations and also are in line with the requirements and obligations under the Act;

Provided that where a Regulated Entity relies on a third party that is part of the same Financial Group, the above condition is not applicable. The Regulated Entity can rely on member of the Financial Group subject to the condition that such member meets the following requirements:-

(i) the Financial Group applies and implements a [35][Group-wide programmes] on customer due diligence and record keeping, which meets the standards set out in the FATF Recommendations; and

(ii) the implementation of Customer Due Diligence and record keeping at the group level are supervised by a financial services regulator or other competent authority in a country.

(d) The third party is not based in a country or jurisdiction assessed as high risk;

(e) No Regulated Entity shall rely on a third party to conduct ongoing monitoring of business relations with customers;

(f) No Regulated Entity shall rely on a third party specifically precluded by the Authority from relying upon;

(g) The Regulated Entity shall document the basis for its satisfaction that the requirements under sub-clause (c) have been met;

(h) The reliance on Third Party shall also be subject to the conditions that are specified in rule 9 (2) of the Rules and shall be in accordance with the regulations and circulars/guidelines issued by Authority from time to time; and,

(i) The Regulated Entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

Guidance Note: -

(1) In a Third-Party reliance scenario, the Third Party will typically have an existing relationship with the customer that is independent of the relationship to be formed by the customer with

[35] Substituted for word "group-wide policy" vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

the relying Regulated Entity. The third party will therefore perform the CDD measures on the customer according to its own AML/CFT policies, procedures and controls.

(2) Obtaining records or information of the client due diligence under sub-clause (a) above, means obtaining all relevant CDD information, and not just basic information such as name and address.

(3) For the avoidance of doubt, it is clarified that a Regulated Entity is not required automatically to obtain the underlying certified documents used by the third party to undertake its CDD. A Regulated Entity shall, however, under sub-clause (b) above, ensure that the certified documents are readily available from the third party on request.

(4) The Regulated Entity shall take appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in.

(5) Where a particular jurisdiction's laws (such as secrecy or data protection legislation) would prevent a Regulated Entity from having access to CDD information upon request without delay, the Regulated Entity should undertake the relevant CDD itself and should not rely on the third party.

(6) If a Regulated Entity is not reasonably satisfied that a customer or Beneficial Owner has been identified and verified by a third party in a manner consistent with these Guidelines, the Regulated Entity shall immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.

(7) When assessing under Clause 6.2 (c) above, a Regulated Entity shall consider following factors including, among other things:

(a) mutual evaluations, assessment reports or follow-up reports published by FATF and other International Organisations;

(b) contextual factors such as political stability or the level of corruption in the jurisdiction;

(c) evidence of recent criticism of the jurisdiction, including in:

(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML regime by organisations referred to in (a); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations.

CHAPTER-VII

CORRESPONDENT BANKING AND WIRE TRANSFERS

7. Correspondent Banking

7.1. A Regulated Entity shall have a policy approved by its Governing Body, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions namely: -

(a) assessment of the suitability of the respondent bank by taking the following steps:
   (i) gather adequate information about the respondent bank to fully understand the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
   (ii) determine from the available sources, the reputation of the respondent bank and the quality of supervision over it, including whether it has been the subjected to any ML/TF investigation or regulatory action; and,
   (iii) assess the respondent bank's AML/CFT controls and ascertain whether they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;

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

(c) obtain approval from the Senior Management before providing correspondent banking or similar services to a respondent bank.

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

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

(f) Correspondent relationship shall not be entered into with a bank which is a Shell Financial Institution.

(g) It shall be ensured that the correspondent banks do not permit their accounts to be used by bank which is a Shell Financial Institution.

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

(i) It shall be ensured 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.

Wire Transfers

7.2. This Clause shall apply to a bank or Regulated Entity when it sends funds by wire transfer or when it receives funds (including serial payments and cover payments) by wire transfer on the account of the wire transfer originator or the wire transfer beneficiary, but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary, respectively.

[36][7.2A.The Regulated Entity shall verify the information pertaining to its customer where there is a suspicion of ML/TF.]

[37][7.2B.All Financial Institutions shall transact [38][and] receive all monetary consideration (i.e. funds/fees/amount) only through an account maintained with a Banking Unit in the IFSC.]

7.3. A Regulated Entity shall monitor payment messages to and from high risk countries or jurisdictions, as well as transactions with high risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.

7.4. Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or a terrorist entity, the Regulated Entity shall block, reject or freeze assets of these terrorists or terrorist entities immediately.

7.5. Where there are positive hits arising from name screening checks, they should be escalated to the Principal Officer. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and be documented.

7.6. A Regulated Entity shall not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another Regulated Entity in the payment process.

Guidance Note: -

(1) Clause 7.2. is not intended to cover: -

(i) any transfer that flows from a transaction carried out using a credit, charge, debit or prepaid card for the purchase of goods or services, so long as the credit, charge, debit or prepaid card number accompanies all transfers flowing from the transaction.

(ii) transfers and settlements between the entities, where both the originator and the beneficiary are Regulated Entities acting on their own behalf.

(2) Clause 7.2. shall apply when a credit, charge, debit or prepaid card is used as a payment system to effect a person-to-person wire transfer. In such a case, the necessary information should be included in the message for such transactions.

---

[36] Inserted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).
[37] Clarified vide Circular dated November 18, 2024 (the circular can be accessed at: https://shorturl.at/XCzX2).
[38] Substituted for the words "or", vide Circular dated January 02, 2026.

7.7. Responsibility of the Ordering Institution

7.7.1. Identification and Recording of Information

Before effecting a wire transfer, every bank that is an ordering institution shall: -

(a) identify the wire transfer originator and verify his or its identity; and

(b) record adequate details of the wire transfer so as to permit its reconstruction, including but not limited to, the date of the wire transfer, the type and amount of currency transferred and the value date.

7.7.2. Cross-Border Wire Transfers Below or Equal To USD 1000

In a cross-border wire transfer where the amount to be transferred is below or equal to USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique transaction reference number where no account number exists);

(c) the name of the wire transfer beneficiary; and

(d) the wire transfer beneficiary's account number (or unique transaction reference number where no account number exists).

7.7.3. Cross-border Wire Transfers [39][Equal to or] Exceeding USD 1000

(a) In a cross-border wire transfer where the amount to be transferred [40][is equal to or] exceeds USD 1000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer, the information required under Clause 7.7.2. (a) to (d), and any of the following:

(i) the wire transfer originator's residential address;

(ii) registered or business address, and if different, principal place of business, as the case may be;

(iii) the wire transfer originator's unique identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number); or

(iv) the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).

(b) Where several individual cross-border wire transfers from a single wire transfer originator are bundled in a batch file for transmission to wire transfer beneficiaries, a bank shall ensure

[39] Clarified vide Circular dated August 31, 2023 (the Circular can be accessed at https://shorturl.at/l4gOb).
[40] Clarified vide Circular dated August 31, 2023 (the Circular can be accessed at https://shorturl.at/l4gOb).

that the batch transfer file contains below information which are fully traceable within the beneficiary country:

(i) the wire transfer originator information required under Clause 7.7.3, which has been verified; and

(ii) the wire transfer beneficiary information required under Clause 7.7.3.

[41][*Explanation:* For avoidance of doubts, it is clarified that, Clause 7.7.3. (b) shall apply to all Cross- Border Wire Transfers which are bundled in a batch file.]

7.7.4. <u>Domestic Wire Transfers</u>

In a domestic wire transfer, every bank that is an ordering institution shall either: -

(a) include in the message or payment instruction that accompanies or relates to the wire transfer, the following:

(i) the name of the wire transfer originator;

(ii) the wire transfer originator's account number (or unique transaction reference number where no account number exists); and

(iii) any of the following:

(aa) the wire transfer originator's residential or registered or business address or principal place of business (if registered and business addresses are different), as applicable;

(bb) the wire transfer originator's unique national identification number (such as an identity card number, birth certificate number or passport number, or where the wire transfer originator is not a natural person, the incorporation number or business registration number);

(cc) the date and place of birth, incorporation or registration of the wire transfer originator (as applicable).

(b) Include only the wire transfer originator's account number (or unique transaction reference number where no account number exists), provided: -

(i) that these details will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary;

(ii) the ordering institution shall provide the wire transfer originator information set out in Clause 7.7.4. (a) within 3 business days of a request for such information by the beneficiary institution, by the Authority or other relevant authorities; and

(iii) the ordering institution shall provide the wire transfer originator information set out in Clause 7.7.4. (a) above, immediately upon request for such information by law enforcement authorities in India.

[41] Clarified vide Circular dated August 31, 2023 (the Circular can be accessed at https://shorturl.at/l4gOb).

(c) All wire transfer originator and beneficiary information collected by the ordering institution shall be documented. Where the ordering institution is unable to comply with the requirements under Clause 7.7.1. to 7.7.4, it shall not execute the wire transfer.

7.7.5. Responsibility of the Beneficiary Institution

(a) A bank that is a beneficiary institution shall take reasonable measures, including post event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack the required wire transfer originator or required wire transfer beneficiary information.

(b) For cross-border wire transfers, a beneficiary institution shall identify and verify the identity of the wire transfer beneficiary, if the identity has not been previously verified.

(c) A bank that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for determining:

(i) when to execute, reject, or suspend a wire transfer lacking required information related to wire transfer originator or wire transfer beneficiary; and

(ii) the appropriate follow-up action.

7.7.6. Responsibility of the Intermediary Institution

(a) A bank, who is acting as an intermediary institution, shall retain all the required information related to wire transfer originator and wire transfer beneficiary, accompanying the wire transfer.

(b) Where technical limitations prevent the required information related to wire transfer originator or wire transfer beneficiary accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be preserved by the receiving intermediary institution for at least six years [42][*]..

(c) An intermediary institution shall implement appropriate internal risk-based policies, procedures and controls for determining-

(i) when to execute, reject, or suspend a wire transfer lacking required wire transfer originator or wire transfer beneficiary information; and

(ii) the appropriate follow-up actions.

(d) [43][The Intermediary Institution shall be required to take all reasonable measures, consistent with straight-through processing, to identify cross-border wire transfers that lack the information required under clause 7.7.6 (a)of the Guidelines.]

[42] The words "or for such period as prescribed under the applicable laws" Omitted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).

[43] Clarified vide Circular dated August 31, 2023 (the Circular can be accessed at https://shorturl.at/l4gOb).

CHAPTER—VIII

INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

8.1. Internal Policies

A Regulated Entity shall develop and implement adequate internal policies, procedures and controls, taking into consideration its ML/TF risks and the size of business, to help prevent ML/TF, and communicate these to its employees.

Guidance Note:

As internal policies and procedures serve to guide employees, officers and representatives in ensuring compliance with AML/CFT laws and regulations, it is important that a Regulated Entity updates its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

8.2. Compliance

(a) A Regulated Entity shall develop appropriate compliance management, including appointing or designating a Principal Officer at the management level and shall also develop compliance framework.

(b) A Regulated Entity shall ensure that the Principal Officer, as well as any other persons appointed to assist him, is suitably qualified and, has adequate resources and timely access to all customer records and other relevant information which he may require to discharge his functions.

(c) A Regulated Entity shall ensure that the Principal Officer has the necessary seniority and authority within the Regulated Entity to effectively perform his responsibilities.

(d) The responsibilities of the Principal Officer shall include:

(i) carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with these Guidelines;

(ii) promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organization;

(iii) informing employees, officers and representatives promptly of regulatory changes;

(iv) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;

(v) reporting or overseeing the reporting of suspicious transactions;

(vi) advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;

(vii) reporting to Senior Management on the outcome of reviews of the Regulated Entity's compliance with these Guidelines & risk assessment procedures; and

(viii) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Regulated Entity's Senior Management.

(e) The business interests of a Regulated Entity should not interfere with the effective discharge of the above-mentioned responsibilities of the Principal Officer and potential conflicts of interest should be avoided.

(f) To enable unbiased judgments and facilitate impartial advice to management, the Principal Officer should be distinct from the internal audit and business line functions. Where any conflict between business lines and the responsibilities of the Principal Officer arises, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the Regulated Entity's management.

8.3. Audit

(a) A Regulated Entity shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the Regulated Entity's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines.

(b) A Regulated Entity's AML/CFT framework should be subjected to periodic audits. Such audits should be performed not just on individual business functions but also on a Regulated Entity-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would *inter-alia* include —

(i) Determining the adequacy of the Regulated Entity's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(ii) Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee's, officer's and representative's compliance with established AML/CFT policies and procedures; and

(iii) Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the Regulated Entity's business.

8.4. Training and awareness

The Regulated Entity shall: -

(a) provide AML/CFT training to all relevant employees, periodically;

(b) ensure that its AML/CFT training enables its employees to:

(i) comprehend the applicable laws relating to ML/TF, including the Act and Rules;

(ii) understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;

(iii) recognise and deal with transactions and other activities which may be related to ML/TF;

(iv) comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;

(v) have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of the Regulated Entity;

(vi) understand their roles and responsibilities in combating ML/TF, including the identity and duties of the Regulated Entity's Principal Officer and deputy, where applicable; and,

(vii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter VI.

(c) ensure that its AML/CFT training:

(i) is relevant and tailored to the Regulated Entity's activities, including its products, services, customers, distribution channels, business partners, level and nature of its transactions; and

(ii) identifies and indicates the different levels of ML/TF risk and vulnerabilities associated with the matters in sub-clause (c)(i) above.

Guidance Note: -

(1) All new relevant employees of a Regulated Entity should be given appropriate AML/CFT training as soon as reasonably practicable after commencing employment with the Regulated Entity.

(2) The manner of providing AML/CFT training may not necessarily be formal and may include any medium which is considered appropriate.

(3) A relevant employee may include a member of the Senior Management or operational staff, any employee with customer contact or who handles or may handle customer monies or assets, and any other employee who might otherwise encounter ML/TF in the business context.

CHAPTER- IX

RECORD KEEPING

9. Record Keeping

9.1. A Regulated Entity shall maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;

(b) records of customer business relationships (both original and certified copies), which include: -

(i) correspondence of business and other information relating to a customer's account;

(ii) adequate records of transactions to enable standalone transactions to be reconstructed; and

(iii) internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;

(c) notifications made under Clause 10.1. (b);

(d) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications, if made with the FIU;

(f) the documents referred to in Clause 9.4; and

(g) any other matter that the Regulated Entity may be expressly required to record and maintain, under these Guidelines.

9.2. The Regulated Entity shall preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed.

9.3. The Regulated Entity shall provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines.

9.4. Risk Assessment Documents

A Regulated Entity shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information, including: -

(a) the business risk assessment undertaken by them as per Clause 3.1;

(b) how the business risk assessment in (a) was used for the purposes of complying with Clause 4.1. (a);

(c) the risk assessment of its customer undertaken under Clause 4.1. (a) (i); and,

(d) the determination of risk rating made under Clause 4.1. (a) (ii).

Guidance Note: -

(1) A Regulated Entity shall comply with the requirements prescribed under rule 3, 4 and 5, along with any other applicable provisions under the Act, Rules and these Guidelines.

(2) The above records may be kept in electronic format, subject to the condition that such records are readily accessible and promptly made available to the Authority or other law enforcement agency, on demand.

(3) Where the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

(4) The Regulated Entity shall evolve a system for proper maintenance and preservation of records in such a manner that allows:

(a) data to be retrieved easily and quickly whenever required or when demanded by the competent authorities;

(b) the Authority or any other competent authority is able to assess the Regulated Entity's compliance with the applicable laws;

(c) identification of a customer or third party;

(d) it permits reconstruction of any transaction which was processed by or through the Regulated Entity on behalf of a customer or other third party;

9.5. Where the records referred to in Clause 9.1 are kept by a Regulated Entity outside the IFSC, the Regulated Entity shall:

(a) take all reasonable steps to ensure that the records are kept in a manner consistent with these Guidelines;

(b) ensure that the records are easily accessible to it; and

(c) ensure that the records are immediately made available for inspection, when so desired by the Authority.

9.6. All Regulated Entities shall:

(a) verify if there are secrecy or data protection laws that would restrict access without delay to the records referred to in Clause 9.1, by the Regulated Entities, the Authority or the law enforcement agencies of India; and

(b) where such law exists, obtain without delay, the certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons referred in Clause (a) above.

9.7. The Regulated Entities shall be able to convey that they have complied with the training requirements in Chapter VIII through appropriate measures, including the maintenance of relevant training records.

CHAPTER-X

PROCESS OF IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

10.1. Internal reporting requirements

(a) A Regulated Entity shall establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious transactions with respect to potential ML/TF.

(b) A Regulated Entity shall put in place such policies, procedures, systems and controls which ensure that whenever any of its employee, acting in the ordinary course of his employment, either:

(i) knows;

(ii) suspects; or

(iii) has reasonable grounds for knowing or suspecting;

that a person is engaged in or attempting ML/TF, that employee promptly notifies the Principal Officer of the Regulated Entity with all relevant details.

10.2. Indications of Suspicious Transactions

A Regulated Entity can identify suspicious transactions by following these four steps:

(a) Detect a suspicious indicator(s);

(b) Ask the customer questions;

(c) Review customer's records; and

(d) Evaluate the above information.

(a) Detect Suspicious indicators

The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity or lacks a business or apparent lawful purpose.

Guidance Note: -

1) The suspicious indicators act as "red flags" and alerts for the Regulated Entity to pay more attention to a particular customer or transaction(s). These indicators include:

(a) complex, unusual or large transactions that have no apparent economic or lawful purpose;

(b) unusual pattern of transactions that have no apparent economic or lawful purpose;

(c) the transaction (or attempted transaction) does not match the known background, nature and type of customer, including source of funds;

(d) unusual customer behaviour;

(e) Customers whose identity verification seems difficult or clients that appear non-cooperative;

(f) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;

(g) Customers based in high-risk jurisdictions;

(h) Substantial increases in business without apparent cause; or

(i) Attempted transfer of investment proceeds to apparently unrelated third parties.

2) The presence of suspicious indicators does not immediately equate to the criminality or suspicion. Rather, the detection of an indicator especially a combination of indicators should prompt the Regulated Entity to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU-IND as suspicious.

(b) Ask Customer Questions

(i) If one or more suspicious indicators are detected, the Regulated Entity and its employees may ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

(ii) The Regulated Entity shall ensure that when asking such questions, they do not "tip-off" the customer. Instead, questions could be asked using a service approach.

(c) Review Customer's Records

The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. To achieve this, a Regulated Entity shall review its customer's records and consider all information that is already known to it about the customer. This may include:

(i) the customer's usual occupation, business or principal activity;
(ii) the customer's transaction history;
(iii) the customer's risk profile;
(iv) the customer's income level;
(v) the customers source of income as stated during account opening or initial engagement;
(vi) reasons for the transactions as provided by the customer;
(vii) the "relationship" of the customer with the sender or beneficiary of funds;
(viii) the frequency of transactions;
(ix) the size and complexity of the transaction;
(x) the identity or location of any other person(s) involved in the transaction;
(xi) the usual or typical financial, business or operational practices or behavior of customers in the similar occupation or business category; and
(xii) the availability of identification documents and other documentation.

After reviewing as aforesaid if the Regulated Entity finds that the customer's profile has changed, it shall update the customer's profile.

(d)Evaluate Information Collected

(a) A Regulated Entity shall evaluate the:

(i) suspicious indicators,

(ii) information solicited from the customer through questions asked, and

(iii) known information about the customer to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence.

(b) If the Regulated Entity concludes that there are reasonable grounds to suspect that the transaction(s) or attempted transaction(s) is linked to a ML/ TF or any other serious offence, it should report this suspicion to the FIU-IND by completing and submitting a STR.

Guidance Note: -

1) A Regulated Entity should be able to clearly articulate the reasons for its suspicion based on this evaluation. If a Regulated Entity is unable to establish reasonable grounds of suspicion, it must continue monitoring the customer or the business relationship.
2) By monitoring a customer's activity, a Regulated Entity may revert to any of the above steps (detect, ask, review and evaluate) at a later date and find that new facts and context may raise the suspicion to meet the reasonable grounds of suspicion threshold.
3) The requirement to report any suspicious transaction applies to all types of transaction. There is no minimum monetary threshold amount for reporting suspicious transactions. Thus, a transaction considered suspicious should be reported to the FIU-IND regardless of the currency or amount of the transaction.
4) If a Regulated Entity is not able to obtain satisfactory evidence of a customer's identity, the Regulated Entity should not proceed further with the transaction unless directed in writing to do so by the FIU-IND.
5) If the Regulated Entity considers the reasons for the customer's failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it shall report the attempted transaction to the FIU-IND as a suspicious transaction.

REPORTING OF SUSPICIOUS TRANSACTIONS

10.3. Reporting Requirements to Financial Intelligence Unit – India

[44][(1) The name, designation and address of the Designated Director and the Principal Officer shall be communicated to the FIU-IND and the Authority.

[44] Substituted for "A Regulated Entity shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the required information referred to in rule-3 of the Rules and in accordance with the terms of rule-7 thereof." vide Circular dated January 02, 2026.

(2) A Regulated Entity shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the required information referred to in rule-3 of the Rules and in accordance with the terms of rule-7 thereof.]

Guidance Note: -

1) The reporting formats and comprehensive reporting format guide prescribed or released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Regulated Entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file Suspicious Transaction Reports (STR) which FIU-IND has placed on its website, shall be made use of by Regulated Entities which are yet to install/adopt suitable technological tools for extracting STR from their live transaction data.
2) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.

[45][(2A) Regulated entities shall not restrict any transaction in any account merely on the basis of the STR file].

3) Robust software to throw 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.
4) In terms of the Rules, the Regulated Entities are mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND). [46][*]
5) The Regulated Entities shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND.
   (a) Further, in terms of Rules, the Regulated Entities shall inter-alia adhere to the following:

---

[45] Inserted vide Circular date January 02,2026.

46 Omitted vide Circular dated January 02,2026. Prior to omission Guidance Note (4), read as under

"In terms of the Rules, the Regulated Entities are mandated to report information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,

Financial Intelligence Unit-India,

6th Floor, Tower-2,

Jeevan Bharati Building, Connaught Place,

New Delhi-110001,

Telephone: 91-11-23314429, 23314459

Website: http://fiuindia.gov.in"

(i) The Suspicious Transaction Report (STR) shall be submitted [47][promptly on] conclusion that any transaction or a series of transactions that are integrally connected, are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

(ii) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

(iii) The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND;

(iv) Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND.

10.4. Confidentiality of Suspicious Transaction Report (STR)

(a) The Regulated Entities and its employees or agents shall not disclose to any person (including the customer):

(i) that it has reported or will be reporting a suspicious transaction to the FIU-IND;

(ii) that it has formed a suspicion on a particular customer's transaction; or

(iii) any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU-IND.

(b) Disclosure of information on suspicious transactions is only allowed under the following circumstances:

(i) disclosure to an officer, employee or agent of the Regulated Entity for any purpose connected to the performance of that person's duties;

(ii) disclosure to a lawyer for the purpose of obtaining legal advice on the matter;

(iii) disclosure to a supervisory authority (to enable it to carry out its supervisory role); [48][*]

(iv) disclosure in compliance with the court order, [49][or]

(v) [50][disclosure or information sharing among entities in a Financial Group.]

(c) The Regulated Entities and its employees are protected from any civil, criminal or disciplinary action taken against them for reporting a suspicious transaction in good faith.

[47] Substituted for "within 7 days of arriving at a" vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).
[48] The word 'or' omitted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).
[49] Inserted vide Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).
[50] Inserted by Circular dated October 12, 2023 (the Circular can be accessed at https://shorturl.at/LpBeA).

Guidance Note:

1) No Nil reporting needs to be made to FIU-IND in case there are no suspicious/ non – profit organization transactions to be reported. The Regulated Entities shall not put any restrictions on operations in the accounts where an STR has been made. The Regulated Entities and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND.
2) This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the customer at any level.
3) It is clarified that the Regulated Entities, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of the Schedule of the Act, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

10.5. Additional Measures

(a) Lawyers, notaries, accountants, and entities offering such services shall report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the following activities :-

(i) buying and selling of real estate;
(ii) managing of client money, securities or other assets;
(iii) management of bank, savings or securities accounts;
(iv) organization of contributions for the creation, operation or management of companies;
(v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

CHAPTER- XI

COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

11.1. Requirements/obligations under International Agreements Communications from International Agencies –

(a)

The Regulated Entities shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of

individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(i) 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

(ii) 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

The aforementioned lists, i.e., UNSC Sanctions Lists, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Regulated Entities for meticulous compliance.

(b) Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available at https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf

(c) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

[51][(d) The Regulated Entity shall adhere to the countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.]

[52][(e) Regulated Entities shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of

[51] Inserted vide Circular dated November 22, 2024(the Circular can be accessed at https://shorturl.at/4aDkf)
[52] Clarified vide Circular dated October 20,2023 (the Circular can be accessed at https://shorturl.at/XDIH4).

Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (available at https://fiuindia.gov.in/pdfs/AML_legislation/DoR_Section_12A_WMD.pdf).]

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

The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed and compliance with the Order shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

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

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

Explanation: The process referred to in (a) and (b) above, do not preclude Regulated Entities 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 as aforesaid shall be examined, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

11.4. Secrecy Obligations and Sharing of Information:

(a) A Regulated Entity shall maintain secrecy regarding the customer information that arises out of the contractual relationship between it and the customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express consent of the customer.

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

(d) The exceptions to the above obligations shall be as under:

(i) Where disclosure is under compulsion of law;

(ii) Where there is a duty to the public to disclose;

(iii) Where the interest of Regulated Entity requires disclosure; and

(iv) Where the disclosure is made with the express or implied consent of the customer.

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

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

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

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

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

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

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

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

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

(i) updated Guidance Note on FATCA and CRS; and

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

11.6. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR):

(a) In terms of provision of rule 9(1A) of Rules, a Regulated Entity shall capture customer's KYC records and upload on CKYCR within 10 days of commencement of an account-based relationship with the customer in the form and manner as prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) and shall ensure that:

(i) The KYC records to be uploaded are as per KYC Template released by CERSAI.

(ii) Once KYC Identifier is generated by CKYCR, the same is communicated to the Customer.

(iii) It has performed the last KYC verification or has sent updated information in respect of a Customer to CKYCR.

(b) [53][For the purpose of establishing an account-based relationship or for verification of identity of a customer or for undertaking on-going due diligence, the Regulated Entity shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR, and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless –

(i) there is a change in the information of the customer as existing in the records of

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

(i) there is a change in the information of the customer as existing in the records of CKYCR;

(ii) the current address of the customer is required to be verified; and,

(iii) the Regulated Entity considers it necessary in order to verify the id

entity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client." vide Circular dated June 05, 2025 (the Circular can be accessed at https://shorturl.at/4BrTr).

CKYCR; or

(ii) the KYC record or information retrieved is incomplete or is not as per the applicable KYC norms under these Guidelines; or

(iii) the validity period of the downloaded documents has lapsed; or

(iv) the Regulated Entity considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.]

(c) [54][Whenever the Regulated Entity obtains additional or updated information from any customer as per clause (b) above, it shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall then update the existing KYC records of such customer.

(d) The CKYCR shall thereafter inform electronically all the Regulated Entities who have dealt with the concerned customer regarding updation of KYC record of such customer and on receipt of such information, the concerned Regulated Entity shall retrieve the updated KYC records from CKYCR and update the KYC records maintained by them.

(e) The Regulated Entities engaged in the following activities shall adhere to the requirements stipulated under sub-clause (a) to (d) above:

(i) Payment Service Provider;
(ii) Finance Company undertaking core activities (Finance Company- Core);
(iii) IFSC Banking Unit;
(iv) Bullion Trading /Clearing Member;
(v) Broker Dealer;
(vi) Clearing Member;
(vii) Depositary Participant;
(viii) Investment Advisor;
(ix) Fund Management Entity;
(x) General Insurance;
(xi) Life Insurance.]

Guidance Note

[55][(1) Under rule 9A of the Rules, a Regulated Entity shall submit KYC Records to the CKYCR, in case of the Indian nationals. However, such requirement shall not be applicable for a client who is a foreign national.

[54] Inserted vide Circular dated June 05, 2025 (the Circular can be accessed at https://shorturl.at/4BrTr).
[55] Substituted for "Under rule 9A of the Rules, a Regulated Entity is required to submit KYC Records to the Central KYC registry, in case of the Indian nationals. However, this requirement shall not be applicable in case of foreign nationals." vide Circular dated June 05, 2025 (the Circular can be accessed at https://shorturl.at/4BrTr).

(2) Notwithstanding anything provided above, where a Regulated Entity intends to submit the KYC records of a foreign national to the CKYCR, in such case the documents issued by the Government departments of foreign jurisdictions and letters issued by the Foreign Embassy or Mission in India shall be accepted as proof of current address and when this proof of address is accepted, then any of the following OVDs shall be obtained as the proof of identity and address:

(i) Passport;

(ii) Driving License; or

(iii) Voter Identity Card.]

CHAPTER-XII

GROUPS, BRANCHES AND SUBSIDIARIES

12.1. Obligation to develop and ensure implementation of KYC/AML-CFT standards

(a) A Regulated Entity incorporated in an IFSC, shall develop a [56][Financial Group's programmes (Group-wide programmes)] on AML/CFT to meet the requirements of these Guidelines and extend the same to all of its branches and majority owned subsidiaries. [57][These Group-wide programmes] should include:

(i) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;

(ii) an ongoing employee training programme; and

(iii) an independent audit function to test the system.

(b) The Regulated Entity shall communicate the [58][Group-wide programmes] to all its branches and majority owned subsidiaries and ensure its implementation.

(c) Where the KYC/AML-CFT standards in another jurisdiction differ from those specified by the Authority, the Regulated Entity shall require its branch or majority owned subsidiary in that jurisdiction to apply the higher of the two standards, to the extent permitted by the law of that jurisdiction.

---

[56] Substituted for the words 'group policy', vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

[57] Substituted for the words 'The group policies', vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

[58] Substituted for the words 'group policy', vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

(d) Where the law of another jurisdiction does not permit the implementation of KYC/AML-CFT standards that are equivalent to or higher than those that apply to the Regulated Entity incorporated in an IFSC, the Regulated Entity shall: -

(i) inform the Authority in writing; and

(ii) apply appropriate additional measures to prevent the ML/TF risks posed by the relevant branch or subsidiary.

(e) Where the Regulated Entity has a branch or subsidiary in a country or jurisdiction:

(i) For which the FATF has called for countermeasures; or

(ii) It is known to have inadequate AML/CFT measures, as identified by the Regulated Entity for itself or notified by the Authority or other foreign regulatory authorities to the Regulated Entities;

the Regulated Entity shall ensure that its [59][Group-wide programmes] on KYC-AML-CFT standards is strictly observed by the management of that branch or subsidiary.

[60][(f) Financial Groups are required to implement Group-wide programmes for the purpose of discharging obligations under the provisions of Chapter-IV of the Act, Rules and Guidelines.]

12.2. [61][Group Wide Programmes]

A Regulated Entity which is part of a Financial Group must ensure that it:

[62][(a) has developed and implemented Group-wide programmes against ML/TF, including group- wide policies and procedures for sharing of information required for the purpose of CDD and ML/TF risk management;]

(b) has put in place adequate safeguards to protect the confidentiality and use of any information that is exchanged[, including safeguards to prevent tipping-off] between Financial Group entities;

---

[59] Substituted for the words 'group policy', vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).
[60] Inserted vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).
[61] Substituted for the words 'Group Policy', vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).
[62] Substituted for the words 'has developed and implemented its group policies and procedures for the sharing of information between Financial Group entities, including the sharing of information related to CDD and for ML/TF risk management;' vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

(c) remains aware of the ML/TF risks of the Financial Group as a whole, of its exposure to the Financial Group and takes active steps to mitigate such risks;

(d) contributes to a Group-wide risk assessment to identify and assess ML/TF risks for the Financial Group;

(e) [63][provides its Group-wide compliance, audit and AML/CFT functions of customer, account, and transaction information from its branches and subsidiaries, including information and analysis of transactions or activities which appear unusual, if such analysis has been conducted, when necessary for the purposes of ML/TF risk management. Similarly, branches and subsidiaries should receive such information from these group-level functions when it is relevant and appropriate for effective risk management.]

i. Annexure-I

Guidance on CDD Procedure

(Refer Clause 5.4.3)

Part-I

Guidance for identification of the customers

For onboarding customers, the Regulated Entity may obtain such information as may be required under these Guidelines, in addition to that is required under the Act and Rules. The Illustrative list of information to be obtained for onboarding customers is provided below: -

(1) For Individual

(i) Full name, including any aliases;

(ii) Unique Identification Number (such as an Identity card number, passport number, etc.);

(iii) Date of birth;

(iv) Nationality;

(v) Legal domicile;

(vi) Current residential address; (other than a post office box address);

[63] Substituted for the words "provides its Group-wide compliance, audit and AML/CFT functions of customer, account, and transaction information from its branches and subsidiaries, when necessary for the purposes of ML/TF risk management", vide Circular dated November 22, 2024 (the Circular can be accessed at https://shorturl.at/4aDkf).

(vii) Contact details such as personal, office or work telephone numbers.

(viii) Occupation or profession, name of employer and location of activity; (wherever applicable)

(ix) Information regarding the nature of the business to be conducted; (wherever applicable)

(x) Information regarding the origin of the funds; and (wherever applicable)

(xi) Information regarding the source of wealth or income. (wherever applicable).

Guidance Note

The address of a customer should enable a Regulated Entity to physically locate the customer.

(2) For Legal Person or Legal Arrangement

In cases where the customer is a legal person or legal arrangement, the Regulated Entity shall, apart from identifying the customer, shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement. Additionally, the Regulated Entities shall also identify and screen the related parties or connected parties of such customer and should remain apprised of any changes to connected parties. For identification of the connected parties, the Regulated Entities shall obtain the following information of each related or connected party:

(i) full name, including any aliases; and

(ii) Unique Identification Number (such as an Identity card number, passport number, etc.);

Part-II

Guidance for verification of the identity of the customers

(1) Verification of identity through following documents:

(i) Passport;

(ii) Driving license;

(iii) Proof of possession of Aadhar number (for Indian Nationals) ;

(iv) Voter's Identity Card issued by Election Commission of India (for Indian Nationals);

(v) For foreign nationals, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as OVD;

[64][*Explanation 1:* Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by RE/business facilitators.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.]

(2) where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be OVD:

(ii) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

(iii) letter issued by a gazetted officer, with a duly attested photograph of the person.

(3) The Regulated Entity shall ensure that any document used for the purpose of verification of the identity of the customer is an original document.

(4) In case a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where Regulated Entity has no physical contact with the customer or the onboarding of customer is done through non-face to face mode); a Regulated Entity should obtain a copy of the OVD that is certified to be a 'true copy' and such certification may be carried out by any one of the following: -

(i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;

(ii) Notary Public (outside India);

(iii) Court Magistrate (outside India);

(iv) Judge (outside India);

(v) Certified public or professional accountant (outside India);

(vi) Lawyer (outside India);

(vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or

(viii) any other authority as may be specified by the Authority.

(5) The person certifying the OVD should be contactable.

[64] Inserted vide Circular dated January 02, 2026.

(6) Where certification of an OVD is done by the authorised officer of the Regulated Entity, such certified copy should be dated, signed and marked with 'original sighted/verified'.

(7) Where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document shall also be deemed to be Officially Valid Document: utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

(i) property, Municipal tax receipt, city council tax receipt, or such other equivalent document;

(ii) bank account or Post Office savings bank account statement or statement of foreign bank; (applicable only for low-risk customers)

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

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

Provided also that in case the OVD presented by a foreign national does not contain the details of address, the documents issued by the Government departments of foreign jurisdictions [65][and] letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

(8) The illustrative list of documents [66][or the equivalent e-documents thereof] , which may be obtained for verification of the identity of Legal Person or Legal Arrangement, are as follows:

(i) <u>In case of Company</u>

(a) Certificate of incorporation;

(b) Memorandum and Articles of association;

(c) PAN or equivalent document prevalent in the home jurisdiction of the company;

[65] Inserted vide Circular dated January 02, 2026

[66] Inserted vide Circular dated January 02, 2026.

(d) A resolution passed by the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf;

(e) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the company.

(f) [67][the names of the relevant persons holding senior management position; and

(g) the registered office and the principal place of its business, if it is different.]

(ii) <u>In case of Partnership/limited liability partnership</u>

(a) Registration certificate;

(b) Partnership deed/limited liability partnership deed;

(c) PAN or equivalent document prevalent in the home jurisdiction of the partnership firm;

(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the partnership firm;

(e) [68][the names of all the partners and address of the registered office, and the principal place of its business, if it is different.]

(f) Such other documents as may be required by the Regulated Entities to collectively establish the existence of such partnership firm.

(iii) <u>In case of Trust</u>

(a) Registration certificate;

(b) Trust deed;

(c) PAN or equivalent document prevalent in the home jurisdiction of the trust;

(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Trust.

(e) [69][the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust and the address of the registered office of the trust; and

(f) list of trustees and documents as are required for individuals under sub-rule (4) of rule 9 of the Rules and Guidelines for those discharging role as trustee and authorised to transact on behalf of the trust.]

(iv) <u>In case of Unincorporated Associations/ Bodies</u>

(a) Resolution of the managing body of such association/body;

---

[67] Clarified vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).
[68] Clarified vide Circular dated May 23, 2023 (the Circular can be accessed at https://shorturl.at/APtcZ).
[69] Inserted vide Circular dated October 23, 2023 (the Circular can be accessed at https://shorturl.at/vJ2PN).

(b) PAN or equivalent prevalent document in the home jurisdiction;

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

(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transaction on behalf of the Unincorporated Associations/ Bodies.

(e) Such other documents as may be required by the Regulated Entities to collectively establish the existence of such association/body.

Part-III

Various modes of verification of the identity of the customers

(i) Use of Business Facilitators;

(ii) Except for high-risk customers, the following mode of verification may also be considered: -

(a) downloading publicly available information from an official source (such as a regulator's or other official government website).

(b) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases may also be acceptable as a reliable source, provided that the commercial database is recognized for such purpose by the home regulator.

Guidance Note on Business Facilitator: -

1) A Regulated Entity may identify the Business Facilitators in different geographies and shall sign agreements with them with specific terms and conditions ensuring customer secrecy and data protection.
2) A Regulated Entity shall maintain the details of the Business Facilitators assisting the customer, where such services are utilized. The ultimate responsibility for customer due diligence will always be with the Regulated Entities.
3) A Regulated Entity will use Business Facilitators for verifying the information/OVD provided by the customer for opening account.
4) The Business Facilitators shall be domiciled and regulated or registered in jurisdiction not identified in the public statement of FATF as 'High Risk Jurisdictions' subject to a 'Call for Action'; or from any country specified by the Government of India by an order or by way of agreement or treaty with other sovereign governments.

Annexure-II

(refer Clause 5.4.3)

[70][PART-A

V-CIP PROCESS FOR ONBOARDING INDIAN NATIONALS

1.1. Regulated Entities may undertake V-CIP to carry out:

(a) CDD in case of on-boarding of new customers such as an individual, proprietor (in case of a proprietorship firm), authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer.

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

1.2. Regulated Entities opting to undertake V-CIP shall adhere to the following minimum standards:

1.2.1.V-CIP Infrastructure

(i) A Regulated Entity shall comply with the minimum baseline cyber security and resilience framework namely, "*Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs*" dated March 10, 2025 (as amended from time to time), issued by the Authority and all other applicable laws on mitigating or managing Information Technology risks.

(ii) The technology infrastructure for V-CIP shall be housed within the premises of the Regulated Entity or its Financial Group supervised by a financial regulator or a KYC Registration Agency (KRA); and the connections and interactions for undertaking V-CIP shall originate from its own secured network domain.

(iii) Any technology related outsourcing for the process shall be compliant with the standards, as may be specified by the Authority.

(iv) Where cloud deployment model is used, the Regulated Entity shall ensure that the ownership of data in such model rests only with the Regulated Entity or its Financial Group.

(v) Further, the Regulated Entity shall also ensure that all such data including video recordings are transferred to the server(s)/cloud server owned or taken on lease by the Regulated Entity or its Financial Group, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Regulated Entity.

[70] Substituted vide circular dated October 31,.2025 (the Circular can be accessed at https://shorturl.at/JTMP9).

Explanations:

Explanation I : In case the technology infrastructure is housed outside India with the Financial Group, the Regulated Entity shall immediately inform the Authority;

Explanation II **:** In case the data, including video recordings, are transferred to the server(s) or cloud server owned or taken on lease by the Regulated Entity's Financial Group, the Regulated Entity shall have access to such data.

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

(vii) The V-CIP infrastructure/application should be capable of preventing the connections from spoofed IP addresses, using VPNs or proxy servers.

[71][*Explanation.* – For removal of doubt, it is hereby clarified that for resident Indian customers, the IP address shall emanate from India and for Non-Resident Indian it shall emanate either from India or from any one of the following countries where he or she is resident:

a) United States of America;
b) Japan;
c) South Korea;
d) United Kingdom excluding British Overseas Territories;
e) Canada;
f) UAE;
g) Singapore;
h) Australia.
i) European Union excluding Croatia

Provided that the aforementioned jurisdictions shall not be identified by FATF as High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring or by Central Government as high risk jurisdiction for money laundering, terrorist financing or proliferation financing.]

(viii) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp through use of tamper-proof technology. The quality

[71] Substituted for "Explanation. – For removal of doubt, it is hereby clarified that for resident customers, the IP address shall emanate from India and for residents of other countries from the country of United States of America, Japan, South Korea, United Kingdom excluding British Overseas Territories, France, Germany, Canada, UAE and Singapore.", vide Circular dated January 02,2026.

of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(ix) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Regulated Entity. Appropriate artificial intelligence (AI) technology with randomness and anti-deep fake and anti-fraud checks must be used to ensure that the V-CIP is robust.

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

(xi) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration Testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In) or any such other suitably accredited agencies as may be specified. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

1.2.2.V-CIP Procedure

(i) Each Regulated Entity shall formulate a clear policy, workflow and standard operating procedure for V-CIP and ensure adherence to it.

(ii) The V-CIP process shall be operated only by officials of the Regulated Entity, or financial group entity in India supervised by a financial regulator or a KRA Registration Agency under an agreement with specific terms and conditions ensuring customer secrecy and data protection. The Regulated Entity will be ultimately responsible for customer due diligence.

(iii) The official should be specially trained for this purpose and capable of carrying out liveliness check and detect deep-fakes, any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.

(iv) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files,

then there is no need to initiate a fresh session by the Regulated Entity. However, in case of call drop / disconnection, fresh session shall be initiated.

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

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

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

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

(a) Offline Verification of Aadhaar for identification;

(b) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer, or KYC Registration Agency (KRA) set up in IFSC;

(c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

(d) Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by RE.

(ix) A Regulated Entity shall redact or blackout the Aadhaar number in the manner as provided under Part B of Annexure II.

(x) 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 three working days from the date of carrying out V-CIP.

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

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

(xiii) A Regulated Entity shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be

verified online from the database of the issuing authority including through Digilocker. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP. Where a customer does not hold a PAN, an (the Circular can be accessed at https://shorturl.at/XDIH4).thereof shall be obtained.

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

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

(xvi) All matters not specified under the above clauses but required under other statutes such as the Information Technology (IT) Act and the Digital Personal Data Protection Act, 2023 or the rules and regulations made thereunder, shall be appropriately complied with by the Regulated Entity.

1.2.3. V-CIP Records and Data Management

(i) The Regulated Entities shall ensure that the video recordings are stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in these Guidelines, shall also be applicable for V-CIP;

(ii) The activity logs along with the credentials of the authorised person of the Regulated Entity performing the V-CIP shall be preserved.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) Customers (classified as low-risk) through V-CIP

(i) The Regulated Entities may onboard customers, who are Non- Resident Indian ('NRI Customers'), through V-CIP to carry out:

(a) CDD in case of on-boarding of new customers such as individual, proprietor in case of proprietorship, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer;

(b) Updation/Periodic updation of KYC.

Explanations. –

Explanation I: For the purposes of this part, the term "NRI customer" shall refer to a Non-Resident Indian who has been classified as a low-risk customer, by the Regulated Entity in accordance with these Guidelines, and resides in any of the following jurisdictions:

a) [72][United States of America;
b) Japan;
c) South Korea;
d) United Kingdom excluding British Overseas Territories;
e) Canada;
f) UAE;
g) Singapore;
h) Australia;
i) European Union excluding Croatia]

Explanation II: For the avoidance of doubt, it is hereby clarified that the Regulated Entity shall undertake V-CIP only for NRI customers residing in any of the above specified jurisdictions and submits valid proof of current address to that effect.

(ii) While undertaking the V-CIP for onboarding the NRI customers, the Regulated Entity shall ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted to the Regulated Entity.

(iii) The Regulated Entities shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction specified in *Explanation 1* above, for the purpose of verification of the current address.

(iv) [73][Upon verification of the proof of identity of the NRI Customer, in cases where current address of NRI customer cannot be verified from reliable/issuing authority sources, the Regulated Entity shall open the account of the customer in the debit freeze / inactive mode; and shall communicate such customer the manner of activation of debit freeze / inactive account.]

---

[72] Substituted for -
"a) United States of America;
b) Japan;
c) South Korea;
d) United Kingdom excluding British Overseas Territories;
e) France;
f) Germany;
g) Canada;
h) UAE;
i) Singapore."
vide Circular dated January 02,2026.

[73]Substituted for "Upon verification of the proof of identity of the NRI Customer, the Regulated Entity may open the account of the customer in the debit freeze mode; and shall communicate such customer the manner of activation of debit freeze account." vide Circular dated January 02, 2026.

(v) The said debit freeze[74][/ inactive] account of the NRI Customer shall be made operational only upon the receipt and verification of first credit from the bank account provided by such customer as proof of current address at the time of V-CIP onboarding process.]

PART-B

DIGITAL KYC PROCESS FOR INDIAN NATIONALS

2.1. For undertaking CDD of Indian nationals, the Regulated Entities 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) the customer decides to submit his Aadhaar number voluntarily to a bank or any Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act; or

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

(bb) 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 the customer's identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof, as defined in Income-tax Rules, 1962; and

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

Provided that where the customer has submitted,

(i) Aadhaar number under Clause (a) above, to a bank or a Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act, such bank or Regulated Entity 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

[74] Inserted vide Circular dated January 02, 2026.

the Regulated Entity.

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

(iii) an equivalent e-document of any OVD, the Regulated Entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under digital KYC Process as specified under Annexure I of Rules.

(iv) any OVD or proof of possession of Aadhaar number under (a)(i)(bb) above where offline verification cannot be carried out, the Regulated Entity shall carry out verification through digital KYC Process as specified under Annexure I of Rules.

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

Explanation I: Regulated Entity shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

Explanation II: Biometric based e-KYC authentication can be done by authorised official of the Regulated Entity/business facilitators.

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