Bajaj Allianz General Insurance Company Limited

Anti-money Laundering & Counter Financing of Terrorism (AML/CFT) Policy

1. Preamble

Bajaj Allianz General Insurance Company Limited (hereinafter referred to as 'BAGIC' or 'the Company') does not wish to be exploited for money laundering purposes or any kind of financing of terrorist activities. The successful business of Bajaj Allianz General Insurance Company Limited is based on a good reputation and integrity. These assets are guided by high standards of customer identification / verification and customer management (jointly "know your customer"). BAGIC standards in money laundering prevention are outlined in this Policy.

2. Scope

This Policy applies to the activities of all employees (on-role & off-role), individual agents, POSP and other contracting parties/vendors of BAGIC.

3. Money Laundering

This Policy is amended and updated in line with the Insurance Regulatory and Development Authority of India (IRDAI) Master Guidelines on Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT), 2022 vide Master Circular No. IRDAI/IID/GDL/MISC/160/8/2022 dated 1 August 2022 (AML Guidelines) and as amended from time to time.

3.1. What is Money Laundering?

As defined by IRDAI, money laundering is moving illegally acquired cash through financial systems, so that it appears to be legally acquired.

There are perceived to be three common stages of money laundering as detailed below, which are resorted to by the launderers and insurance institutions may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions:

- Placement - the physical disposal of cash proceeds derived from illegal activity,
- Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and
- Integration - creating the impression of apparent legitimacy to criminally derived wealth.

If the layering process succeeds, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. Financial institutions such as BAGIC are therefore placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection. Such disclosures are protected by law, enabling the person with information to be able to disclose the same without any fear and BAGIC likewise need not fear breaching their duty of confidentiality owed to customers.

3.2. Money Laundering Prevention in BAGIC

BAGIC wishes to comply with high standards of ethics and integrity in relation to its business in addition to complying with the relevant legislation pertaining to prevention of money laundering activities and counter-financing of terrorist activities. Appropriate measures will be taken when there are reasonable grounds for suspecting money-laundering or terrorism activities.

It is BAGIC's policy to conduct business only with clients and associates who are involved in legitimate activities and to fully comply with all applicable money laundering prevention laws and regulations, including identification, verification, record-keeping, and reporting requirements.

BAGIC shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

4. Principal Officer and Designated Director

In terms of AML Guidelines, a Designated Director, and the Principal Officer (PO) are required to be appointed by BAGIC to ensure compliance with the applicable provisions of the said guidelines. For this policy, the Designated Director shall be Chief Executive Officer and Managing Director of the Company and Principal Officer shall be Chief Compliance Officer of the Company.

5. Products to be covered:

All products are to be considered for AML KYC and Risk assessment monitoring purposes. However, contracts associated with Reinsurance, Co-insurance and Consortium are exempted from the purview of AML KYC.

6. Policies, Procedures and Controls

It is the aim of BAGIC to prevent any kind of money laundering attempts in relation to the business of the Company, following procedures to be adhered:

6.1. Know Your Customer (KYC)

6.1.1 Considering the potential threat of usage of financial services by a money launderer, BAGIC and its employees, agents etc., would exercise special care to determine the true identity of all customers while (at the time of or before) issuing the policies, on an ongoing basis and also at the time of claim settlement through effective procedures for obtaining proof of identification and residence/address, to ensure that the contracts are not anonymous or under fictitious names.
For determining the identity of the "customer" and the term also refers to the proposer / policyholder, beneficiaries, nominees, and assignees as may be applicable for the purposes of the AML guidelines.

6.1.2 KYC will be applicable at following stages:

- **New Business**: KYC is obtained at the time of in-warding the proposal and post authenticating the KYC policy shall be issued.
- **Refund/Claim:** KYC verification also needs to be carried out at the time of claim/refund stage. In death cases where the payments are required to be made to beneficiaries/ nominees/ legal heirs/assignees necessary due diligence shall be carried out by BAGIC with respect before making the payments. In premium refund/indemnity claims if there is no change in KYC information at the time of periodic updating and the existing documents are compliant with the extant PML Rules, then self-declaration of no change in KYC information will be obtained remotely from customer using registered email or SMS message or digital channels (such as mobile application, online portal) etc. to complete the updating process.
  In case of any change in KYC information of existing customers, scanned or digital documents, indicating changed KYC information, shall be obtained.
- **Ongoing Transactions:** KYC will be verified at the time of processing any endorsement/ claim. If there is no change in KYC information at the time of periodic updating and the existing documents are compliant with the extant PML Rules, then self-declaration of no change in KYC information will be obtained physically or remotely from customer using registered email or SMS message or digital channels (such as mobile application, online portal) etc. to complete the updating process.
  In case of any change in KYC information of existing customers, scanned or digital documents, indicating updated KYC information, shall be obtained.
- **Renewal/Rollover Business**: KYC verification is mandatory from 1st Jan 2024 for all the policies as per risk classification under this policy. If there is no change in KYC information at the time of renewal and the existing documents are compliant with the extant PML Rules, then self-declaration of no change in KYC information will be obtained remotely from customer using registered email or SMS message or digital channels (such as mobile application, online portal) etc. to complete the updating process.
  In case of any change in KYC information of existing customers, scanned or digital documents, indicating changed KYC information, shall be obtained.

6.1.3 BAGIC will take the necessary steps to identify the client and its beneficial owner(s) and take all reasonable measures to verify his/her identity to their satisfaction so as to establish the beneficial ownership and in the event no details are identifiable, the details of the authorized representatives may be collected.

6.1.4 Where a client is an individual person, BAGIC will verify the identity, address and recent photograph in order to comply with provision as specified in sub rule (4) of Rule 9 of the PML Rules, including by using end to end Digital KYC mode as allowed under the applicable regulations.

6.1.5 Under all kinds of Group Insurance policies, KYC of Master Policyholders / Juridical Person / Legal Entity and the respective Beneficial Owners (BO) shall be collected. However, the Master Policyholders under the group insurance shall maintain the details of all the individual members covered, which shall also be made available to the BAGIC as and when required.

6.1.6 Methods by which the Company may carry out the KYC verification:

i. Aadhaar based KYC through Online Authentication Or
ii. Aadhaar based KYC through Offline verification, Or
iii. Digital KYC as per PML Rules, Or
iv. Video Based Identification Process (VBIP) Or

v. KYC identifier allotted to the client by the CKYCR, Or
vi. Officially Valid documents AND PAN/Form 60 (wherever applicable) and any other documents as may be required by the insurer.
Any other method prescribed under the law.

6.2. **Due Diligence**

6.2.1. Simplified Client due diligence (CDD) is conducted all kinds of policies at the time of issuance by obtaining valid KYC documents.

6.2.2. Enhanced Due Diligence (EDD) shall be conducted for high-risk categories of customer. BAGIC should examine, as far as reasonably possible, the background and purpose of all complex, unusual patterns of transactions, which have no apparent economic or lawful purpose.

6.3. Negative list of persons/customers:

The Company shall maintain and update on an ongoing basis, a separate list of negative customers who have indulged in any activity/act prohibited under law including committing frauds of any nature. The Company shall not enter a contract with any customer whose identity matches that of any person whose name has been updated on the negative list. A negative customer includes, but is not limited to:

6.3.1. An Individual/entity notified under Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA): A customer whose identity matches with any person in the:

- UN sanction list or with banned entities/designated individuals or entities and those reported to have links with terrorists or terrorist organizations.
- Designated individuals/ entities, such individuals/entities who are subject to UN sanction measures under UNSC Resolutions.
- Individuals/persons whose name/particulars is appearing in designated sanction list under Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005.

6.3.2. Those individuals/persons whose name is appearing in the list of Banned Organizations/Individuals published by Central Govt – Ministry of Home Affairs.

6.3.3. Fraudulent customers (established fraud).

6.3.4. Negative list of persons/ individuals as provided by IRDAI, if any.

The alternate procedures for identification of customers and his/her income are detailed in **Annexure I and II.**

7. Risk Assessment/ Categorization

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction, etc. As such, the Company would apply due diligence measures on each of the customers on a risk sensitive basis. The basic principle enshrined in this approach is that the Company should adopt an enhanced customer due diligence process for higher risk categories of customers.

In the context of our very large base of customers and the significant differences in the extent of risk posed by them, the Company classifies the customers into high risk and low risk. The basis for such a classification is as follows:

7.1 Low risk customers:

Low risk customers would be those individuals and entities whose identities can be easily identified and transactions in whose accounts by and large conform to the known profile. Illustrative examples of low-risk customers are:

- Salaried employees (Private & Public Sector),
- People belonging to lower economic strata of the society (Contract employees, daily wage, factory workers, self-employed persons etc.),
- Corporate Customers (Company registered under the Companies Act, 1956/2013, which includes private, public, one-person company),
- Limited Liability Partnership registered under The Limited Liability Partnership Act, 2008,
- Partnership Firm under Partnership Act, 1932.

Simplified client due diligence will be conducted for low risk customers

7.2 High risk customers:

High risk customers are predominantly those types of customers where required details for KYC verifications are not centrally available and / or are not available in the public domain. Illustrative examples of high-risk customers are:

- Non-residents, including such individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime,
- Trust, charities, NGO's, Societies, and organizations receiving donations,
- Foreign Companies originating from Sanction countries having shareholding or beneficial ownership,
- Partnership Firms where identity is not available in public domain,
- Politically Exposed Persons and
- Those with dubious/negative reputation as per public information available.

For high-risk customer, BAGIC employee shall take necessary steps to examine one or more of the following to carry out the customer's due diligence:

- Background and purpose of the transaction especially those which do not have apparent economic or visible lawful purpose. The Company shall examine and maintain written findings in highly suspicious cases for the purpose of assisting competent authorities,
- Insurable interest,
- Source of premium payment,
- KYC documents may be available.

7.3 The above-mentioned lists are only illustrative. In all such cases, enhanced due diligence will be carried out by the Compliance department and accordingly approval will be given.

8. **Contracts with Politically Exposed Persons (PEPs)**

Politically Exposed Persons (PEP): shall include persons identified under regulatory requirements to be a PEP, this includes, but is not limited to

- Politicians, Government Officials & Legislative Bodies: An example is a Member of Parliament.
- Executive Bodies: A PEP could range from the head of state down to the assistant ministers.
- Diplomatic Roles: Ambassadors or chargé d'affaires would be considered PEPs.
- Judiciary Bodies: Key people working within supreme courts, constitutional courts, or high-level judicial bodies.
- State-Owned Enterprises: Public Organizations & Institutions, Family members & close associates.

The Company shall lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are close relatives of PEPs where such information is available. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner (s).

9. Monitoring and Reporting of Cash Transactions

9.1. Premium / proposal deposit exceeding Rs. 50,000/- should be remitted through cheques, demand drafts, credit card or any other banking channels. Collection of premiums / proposals deposits in cash beyond Rs. 50,000/- per transaction is permitted only subject to the customer quoting the PAN. The Company shall verify the authenticity of the PAN of the person or entity funding the premium / proposal deposit on an insurance policy.

9.2. If any Integrally connected cash transactions exceed Rs.10 lakhs in a calendar the same shall be reviewed from the angle to suspicious activities and same shall be reported to FIU-India by 15th of next succeeding month.

10. Monitoring and Reporting of Suspicious Transactions

Suspicious transaction means a transaction which gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or appears to be made in circumstances of unusual or unjustified complexity; or appears to have no economic rationale or Bonafide purpose.

All suspicious transactions for AML must be monitored. The Company shall report all suspicious transactions as defined under clause 3.16 of the AML Guidelines irrespective of the monetary value involved in such transactions.

An illustrative list of such transactions as suggested by IRDAI is given below:

- Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information,
- Cash or Demand Draft or combination of both based suspicious transactions for payment of premium over and above Rs. 5,00,000/- (Rupees Five Lakhs only) in a calendar month and If the aggregate number of receipts exceeds 3 from a single person towards payment of any nature under all the insurance policies or proposals under which such person is the Policy Owner or Proposer or Assignee, an alert is triggered
- Assignments to unrelated parties without valid consideration,
- Request for a purchase of policy in amount considered beyond his apparent need,
- Policy from a place where he does not reside or is employed,
- Unusual terminating of policies and refunds,

- Frequent request for change in addresses,
- Inflated or totally fraudulent claims e.g. by arson or other means causing a fraudulent claim to be made to recover part of the invested illegitimate funds,
- Overpayment of premiums with a request for a refund of the amount overpaid.
- Suspicious profile of the customer is observed.
- Premium payment or attempts for payment made by unrelated third party (irrespective of the mode) with no economic rationale or any justified reasons.
- List of Policies issued to entities/persons of entities who are barred/disqualified by Financial Sector Regulators/MCA

BAGIC to report the suspicious transactions immediately on identification. When such transactions are identified post facto the contract, it must be reported to FIU-IND within 7 working days of identification. At any point of time, where Principal Officer no longer satisfied about the identity and the transaction made by the customer, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND) if it is satisfied that the transaction meets the criteria specified above. If any order/notice received from the FIU-IND/Authorities on reported transactions, based on the instructions, the insurance policies will be freezed/unfreezed by the Company. Details of STR shall be strictly confidential. However, Confidentiality requirement does not inhibit information sharing among group entities subject however to adherence to the applicable laws/regulations.

11. Submission of Data on AML/CFT Guidelines

As per revised Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT), 2022 dated August 1, 2022, the Company shall submit annual compliance certificate in the prescribed format within 45 days of end of Financial Year.

12. Record Keeping

12.1. As per Rule 5 of the PML rules, BAGIC, its Designated Director, Principal Officer, employees are required to maintain the information/records of types of all transactions as well as those relating to the verification of identity of customer for a period of five years from the date of transaction. Records pertaining to all other transactions, for which BAGIC are obliged to maintain records under other applicable Legislations/Regulations/Rules to retain records as provided in the said Legislation/Regulations/Rules but not less than for a period of five years from the date of end of the business relationship with the customer.

12.2. BAGIC will maintain the record in electronic form and/or physical form. In cases where services offered by a third-party service providers are utilized, BAGIC shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data, the physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored, and recorded.

12.3. Specific procedures for retaining internal records of transactions both domestic and international shall be maintained to comply swiftly with information requests from the competent authorities. Such records shall be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) to provide, if necessary, evidence for prosecution of criminal activity. In the case of long-term insurance,

full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity, for a period of at least five years after that settlement.

12.4. The customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

12.5. BAGIC shall ensure maintenance of records for the said period as per the prescribed formats and shall furnish the same to the Principal Officer as and when called for by him. BAGIC shall ensure that systems and resources are in place at all times to ensure the same.

12.6. The background, including all documents /office records /memorandums pertaining to such transactions, as far as possible, shall be examined by the Principal officer for recording his findings. These records are required to be preserved for ten years (as against the requirement of five years mentioned under the PML guidelines). Directors, officers, and employees (permanent and temporary) are prohibited from disclosing the fact that a Suspicious Transactions Report or related information of a policy holder/prospect is being reported or provided to the FIU-IND.

13. Responsibilities

13.1. Safeguards

13.1.1. BAGIC shall put in place appropriate safeguards suited to its respective business and customers against money laundering and against fraudulent activities to the detriment of the Company. In the event of dubious or unusual practices in the light of experience or knowledge of money laundering methods, the company shall investigate these in the context of the current business relationship and individual transactions.

13.1.2. The Company shall make all necessary arrangements to ensure that the organization has a sound and proper money laundering prevention safeguard. The ultimate responsibility for the implementation as well as the functioning and effectiveness of the money laundering prevention safeguards remains with the Heads of various department (wherever applicable) even if individual managers have been assigned specific areas of responsibility.

13.1.3. The Branch Managers/Area Managers/Zonal Managers and Regional Managers are also responsible for and required to ensure that the Board approved AML program is being implemented effectively, including monitoring compliance by the company's insurance agents with their obligations under the program.

13.2. Employees / Agents / Corporate Agents / Contracting Parties/Vendors

13.2.1. It is mandatory for all employees / agents / intermediaries / contracting parties/vendors to follow AML policy and must report violations of this policy / guidelines by another employee / agent / intermediaries / contracting parties/vendors to the Principal Officer (Compliance.Officer@bajajallianz.co.in). The PO will review such cases. If it is

determined that the reported activity involves known or suspected money laundering, other criminal activity, or that the transaction is otherwise suspicious, it will be reported by the PO to the Financial Intelligence Unit-India (FIU-IND) set up by the Government of India for further investigation and action in the form of Suspicious Transaction Reports (STR).

13.2.2. Initiate appropriate actions against defaulting intermediaries /representative of BAGIC, who expose BAGIC to AML/CFT related risks on any occasions and the details would be reported to IRDAI for further action.

13.2.3. The list of rules and regulations covering performance of intermediaries /representative of BAGIC must be put in place. A clause should be added making KYC norms mandatory and specific process document can be included as part of the contracts.

13.2.4. Necessary steps will be taken to secure compliance, including when appropriate, terminating the business relationship with such an agent/intermediary.

14. Recruitment and Training of Employees/Agents/Intermediaries

14.1. The agents / other intermediaries, etc. would be monitored for sales practices followed by Sales Distribution Channels and if any unfair practice is being reported then action would be taken after due investigation.

14.2. Periodic risk management reviews would be conducted to ensure adherence to laid down process and ethical and control environment.

14.3. Adequate screening mechanism as an integral part of BAGIC personnel recruitment/hiring process.

14.4. Instruction Manuals on the procedures for selling insurance products, customer identification, record-keeping, acceptance and processing of insurance proposals, issue of insurance policies will be set out.

14.5. The concept of AML would be part of in-house training curriculum for agents / others.

14.6. The specific document with respect to KYC norms will be included as part of the contracts with agents.

14.7. BAGIC has on-going AML/CFT training programme for all new employee frontline staff, processing staff, administration/operation supervisor and managers, staff dealing with new customers and claims conducted by inhouse training team. The frontline staff is specially trained to handle issues arising from lack of customer education.

14.8. Records of training imparted to staff in the various categories should be maintained by the respective training team.

15. Sharing KYC information with Central KYC Registry (CKYCR)

15.1. Government of India has notified the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

15.2. Where a customer submits a “KYC identifier” for KYC, BAGIC shall retrieve the KYC records from CKYCR. In such case, the customer shall not submit the KYC records unless there is a change in the KYC information required by Insurers as per Rule 9(1C) of PML Rules.

15.3. If the KYC identifier is not submitted by the client / customer, Operation team of BAGIC search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the client/ customer, if available.

15.4. If the KYC identifier is not submitted by the client/customer or not available in the CKYCR portal, frontline staff shall capture the KYC information in the prescribed KYC Template meant for “Individuals‟ or “Legal Entities‟, as the case may be.

15.5. Operation team shall file the electronic copy of the client’s KYC records with CKYCR within 10 days after the commencement of account-based relationship with a client/ Customer (both Individual/ Legal Entities) only in case of physical or scanned copy of the documents being submitted and upon duly filled CKYC form received from the customers.

15.6. Once “KYC Identifier” is generated/ allotted by CKYCR, the operation team shall ensure that the same is communicated immediately to the respective policyholder in a confidential manner, mentioning its advantage/ use to the individual/legal entity, as the case may be.

15.7. The following details need to be uploaded on CKYCR if Verification/Authentication is being done using Aadhaar:

For online Authentication,
a) The redacted Aadhar Number (Last four digits)
b) Demographic details
c) The fact that Authentication was done.

For offline Verification
a) KYC data
b) Redacted Aadhaar number (Last four digits).

15.8. At the time of periodic updating, it is to be ensured that all existing KYC records of individual/legal entity customers are incrementally uploaded as per the extant CDD standards. BAGIC shall upload the updated KYC data pertaining to all policies against which “KYC identifier” are yet to be allotted/generated by the CKYCR.

15.9. BAGIC will not use the KYC records of the client obtained from Central KYC Records registry for purposes other than verifying the identity or address of the client and will not transfer KYC records or any information contained therein to any third party unless authorized to do so by the client or IRDAII or by the Director (FIU-IND).

16. Internal Control / Audit

The Internal Audit Department would verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities based on overall risk assessment. The Company shall also upgrade its questionnaire and system from time-to-time in accordance with the extant PMLA and PML Rules. The reports will specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary to strengthen the policy and implementation aspects. Exception reporting under AML policy should be done to Audit Committee of the Board.

17. Outsourcing:

The Company shall not outsource any activities pertaining to compliance with AML and KYC requirements under this policy save and except, KYC verification carried out through third party service providers as prescribed under IRDAI Master Guidelines on Anti-Money Laundering / Counter Financing of Terrorism (AML /CFT), 2022 dated 1 August 2022 as amended from time to time

18. Applicability

The various parts of this policy become applicable as per dates mentioned in various IRDAI Circulars. This policy is as per the extant provisions of applicable laws, rules and regulations and would be reviewed by the Board of Directors on annual basis. Any changes therein will require approval by the Designated Director based on recommendation of the Principal Officer, to the extent applicable, shall be incorporated into this policy, which would be reported to the Board on annual basis.

The said policy is available for the employees' ready reference on https://www.bajajallianz.com/download-documents/other-information/Anti-Money-Laundering-Policy.pdf

(End of the Policy)

Annexure – I
Customer Identification Procedure
Any one document to be obtained from Customers.

Risk Classification	Customer	Documents
Low Risk	Individuals	POI: PAN is a mandatory requirement (Form 60 declaration in case the customer does not hold the PAN on specific conditions) POA: Utility Bill/Bank Passbook (issued not less than 2 months)
Low Risk	Juridical Person (Including Group Administration)	POI: PAN/ TAN is a mandatory requirement POA: GST Certificate/ Registration certificate/Incorporation Certificate
High Risk	Individuals	POI: PAN is a mandatory requirement (Form 60 declaration in case the customer does not hold the PAN on specific conditions) POA: Passport/OCI Card *EDD: Reg. Agreements/Declarations
High Risk	Juridical Person (Including Group Administration)	POI: PAN/TAN is a mandatory requirement POA: GST Certificate/ Registration certificate/Incorporation Certificate EDD: Declaration from the entity on their letter head sealed and signed

Note: *No further document required as proof of address if proof of identity contains address*
POI: Proof of Identity, POA: Proof of Address, EDD: Enhance Due Diligence

Other Valid Documents:

Individual	Juridical Person (Including Group Administration)
• Passport • Driving License • Voter's Identity Card • Job Card issued by NREGA • Aaadhar (in case the customer does not want to share the Aadhar they may submit any of the documents from the OVD list below for address proof) • Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number • Any other document as notified by the Central Government in consultation with the Regulator, Letter from a recognized public	• Verification of legal status of the legal entity/person: through CKYC • KYC of the Authorized person who will be acting on behalf of the entity: same for individual person • KYC of the beneficial owner • Certificate of incorporation/registration and Memorandum & Articles of Association • Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account or Partnership Deed or Trust Deed • Power of Attorney granted to its partners, managers, officers or

authority or public servant verifying the identity and residence of the customer	employees to transact business on its behalf

Annexure - II

Income Proofs

Standard Income proofs:

- Income tax assessment orders/Income Tax Returns
- Employer's Certificate
- Audited Company accounts
- Audited firm accounts and Partnership Deed

Non-standard Income Proofs:

- Chartered Accountant's Certificate
- Agricultural Income Certificate
- Agricultural-land details & Income assessments
- Bank Cash-flows statements, Pass-book

Note: The list is only illustrative and not exhaustive

***

Version 1 approved by the Board of Directors on 5 May 2006
Version 2 approved by the Board of Directors on 27 November 2006
Version 3 approved by the Board of Directors on 25 September 2009
Version 4 approved by the Board of Directors on 12 February 2010
Version 5 approved by the Board of Directors on 31 January 2012
Version 6 approved by the Board of Directors on 10 May 2013
Version 7 approved by the Board of Directors on 16 January 2018
Version 8 approved by the Board of Directors on 16 January 2019
Version 9 approved by the Board of Directors on 14 January 2022
Version 10 approved by the Board of Directors on 24 January 2023
Version 11 approved by the Board of Directors on 23 January 2024
Version 12 approved by the Board of Directors on 18 October 2024