



**POLICY ON KNOW YOUR CUSTOMER NORMS & ANTI-
MONEY LAUNDERING MEASURES**

(KYC & AML Policy)

VERSION CONTROL

Version Control Number	Author	Date Created / updated	Date Effective	Version Description
V1	Jitendra Bhati VP – Compliance & Secretarial	08 September 2017	08 September 2017	Adoption
V2	Priyal Shah	29 March 2019	29 March 2019	Incorporate amendments as per circular NHB(ND)/DRS/Policy Circular No.94/2018-19 dated March 11, 2019
V3	Priyal Shah	08 August 2019	08 August 2019	Incorporate amendments as per RBI Master Direction - Know Your Customer (KYC) Direction, 2016
V4	Priyal Shah	17 June 2020	17 June 2020	Amendment due to extension of KYC norms to HFCs
V5	Nidhi Sadani	11 August 2022	11 August 2022	Amendment in KYC Norms
V6	Nidhi Sadani	25 July 2023	25 July 2023	Incorporate amendment as per Master Direction - Know Your Customer (KYC) Direction, 2016

1. INTRODUCTION

The Reserve Bank of India (RBI) has vide Know Your Customer (KYC) Direction, 2016 (RBI Directions), issued comprehensive guidelines with regard to Know Your Customer (KYC) norms to be followed by Housing Finance Companies (HFC's) and measures to be taken in regard to Anti Money Laundering (AML) and Combating Financial Terrorism (CFT).

Accordingly, HFC's are required to put in place a comprehensive policy framework on 'KYC norms and AML measures', duly approved by their Board of Directors. This policy document has been prepared in line with the RBI Directions, the Prevention of Money-Laundering Act, 2002 (PMLA) and Rules made thereunder, and incorporates the Company's approach towards matters related to KYC, AML and CFT issues.

The Board of Directors of IndoStar Home Finance Private Limited ('IndoStar' or 'the Company') have adopted this Policy on Know Your Customer Norms & Anti-Money Laundering Measures ('Policy') in accordance with the various directions, guidelines, circulars and notifications issued by the RBI, the PMLA and Rules made thereunder, and it is to be read in conjunction with and shall stand auto-corrected with related operational guidelines issued or any changes / modifications which may be advised from time to time by the RBI and/or other regulators. Terms not defined in this Policy shall unless contrary to the meaning thereof have meaning as assigned to them in the RBI Directions, PMLA and Rules made thereunder, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and Aadhaar and other Laws (amendment) Ordinance, 2019.

2. OBJECTIVES OF THE POLICY

The RBI Directions aim at preventing HFC's from being used, intentionally or unintentionally, by criminal elements for money laundering activities including committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism.

The RBI Directions, PLMA and Rules made thereunder also mandate making reasonable efforts to determine the true identity and beneficial ownership of Customers, source of funds, the nature of Customer's business, etc. which in turn helps the Company to manage its risks prudently.

Accordingly, the main objective of this Policy is to enable the Company to have positive identification of its Customers and put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws / laid down procedures and regulatory guidelines.

3. APPLICABILITY, SCOPE AND RESPONSIBILITY

The Policy is applicable to all categories of products and services offered by the Company, and to all branches and offices of the Company.

The Company being a HFC, some of the provisions as specified in the RBI Directions, PMLA and Rules made thereunder may not be strictly applicable to the Company.

The Management Committee of the Company shall ensure compliance with this Policy, the RBI Directions, PMLA and Rules made thereunder, with the assistance of the Designated Director and the Principal Officer. The Management Committee shall issue detailed operational guidelines for implementation of this Policy, the RBI Directions, the PMLA and Rules made thereunder.

The Management Committee shall submit quarterly audit notes and compliance with respect to this Policy, to the Audit Committee of the Board.

For the purpose of this Policy, a Customer shall mean a person who is engaged in a financial transaction or

activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

4. Customer Acceptance Policy

The Company shall ensure the following while accepting and dealing with its Customers:

- No transaction is initiated in anonymous or fictitious/ benami name(s).
- The Company shall carry out customer identification and customer due diligence procedure before initiating any transaction. In case the Customer transacts in joint name, customer identification and customer due diligence procedure shall be carried out for all individuals / entities involved.
- For the purpose of risk categorisation of Customer, Company shall obtain the relevant information from the Customer at the time of transaction.
- The Company shall not initiate a transaction or terminate an existing transaction where the Company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the Customer or non-reliability of the data/information furnished to the Company. It shall be necessary to have suitable built in safeguards to avoid harassment of the Customer. Decision to terminate a transaction shall be taken at a reasonably high level after giving due notice to the Customer explaining the reasons for such a decision.
- Necessary checks before initiating a new transaction so as to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
- The Company shall prepare a profile for each new Customer based on risk categorisation. The Customer profile may contain information relating to Customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the Company. However, while preparing Customer profile, the Company shall take care to seek only such information from the Customer which is relevant to the risk category and is not intrusive. The Customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the Customer.
- Adoption of Customer acceptance policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.
- Where Goods and Services Tax (GST) details are available from the customer, the Company shall verify GST number from the search/verification facility of the issuing authority.

5. Customer Identification Procedure (CIP) and Customer Due Diligence (CDD)

Customer identification is carried out to verify identity of the Customer by using reliable and independent source of documents, data or information to ensure that the Customer is not a fictitious person. Company shall conduct CIP and CDD at the time of commencement of an account-based relationship with the Customer, when there is a doubt about the authenticity or adequacy of the Customer identification data it has obtained, and selling third party products as agents.

The Company shall obtain sufficient information necessary for identification and due diligence to establish, to its satisfaction, the identity of each Customer including the identity of the beneficial owner and authorized signatory acting on behalf of any non-natural person, whether regular or occasional, and the purpose of the intended nature of business relationship. Besides risk perception, the nature of information/documents

required would also depend on the type of Customer (individual, corporate etc). The illustrative list of such information/documents to be obtained from Customer for identification and due diligence is provided at **Annexure – I**. Further, in case any other document is obtained from the customer for the aforesaid purpose then a declaration in that regard will be taken from the customer.

Where a customer submits a KYC Identifier to the Company, with an explicit consent to download records from Central KYC Records Registry (“CKYCR”), then the Company shall retrieve the KYC records online from CKYCR in prescribed manner.

The Company shall capture / obtain the KYC information for submitting with the Central KYC Records Registry in the prescribed KYC templates for individuals and legal entities, in prescribed format.

The Company may to its satisfaction rely on customer due diligence done by a third party, subject to conditions mentioned in the RBI Directions, PMLA and Rules made thereunder.

Decision-making functions of determining compliance with KYC norms shall not be outsourced.

The Company will perform appropriate, specific and where necessary, enhanced due diligence on its Customers that is reasonably designed to know and verify the true identity of its Customers and to detect and report instances of criminal activity, including money laundering or terrorist financing.

The procedures, documentation, type of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations, etc.) between the Company and the Customer and the risk profile of the Customer. Customers / Beneficial owners who are Politically Exposed Persons shall be subjected to enhanced due diligence.

The Company shall take all reasonable measures to ascertain and verify the true identity of all Customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks.

The Management Committee shall, as and when required, provide appropriate relaxation for continued operation of transaction of Customers who, owing to injury, illness or infirmity on account of old age or otherwise and such like causes, are unable to submit PAN or Form 60.

Periodic Updation:

- Customer identification and customer due diligence documents shall be updated periodically. Such updation shall be carried out at least once at following time intervals and manner:
 - (i) Low Risk Customers: 10 years
 - (ii) Medium Risk Customers: 8 years
 - (iii) High Risk Customers: 2 years
- The time limits prescribed above would apply from the date of initiation of transaction / last KYC verification.
- Save as otherwise provided in this Policy, the instructions or procedure for customer identification and customer due diligence shall mutatis mutandis apply in case of Periodic Updation.

6. Risk Management

The Company shall classify its Customers into various risk categories, and based on the assessment and risk

perception decide on customer identification and due diligence procedure to be followed. The illustrative list of such risk categorisation is provided at **Annexure – II**.

Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of Customer and his clients, mode of payments, volume of turnover, social and financial status, ability to confirm identity documents through online or other services offered by issuing authorities etc. to enable categorization of Customers into low, medium and high risk. The risk categorisation of a Customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the Customer.

Documentation requirements and other information to be collected in respect of different categories of Customers will depend on perceived risk and keeping in mind the requirements of PMLA and guidelines issued by RBI / National Housing Bank, from time to time.

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters. The Company shall carry out money laundering and terrorist financing risk assessment exercise periodically to identify, assess and take effective measures to mitigate its money laundering (ML) and terrorist financing (TF) risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. While assessing the ML/TF risk, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time. Further, the internal risk assessment carried out by the Company should be commensurate to its size, geographical presence, complexity of activities/structure, etc.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and the Management Committee shall adopt and put in place policies, controls and procedures in this regard.

Report / update on the Periodic risk assessment carried out by the Company shall be placed before the Audit Committee.

Company's internal audit and compliance functions shall play an important role in evaluating and ensuring adherence to the KYC policies and procedures, under the directions of the Management Committee. Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and any lapse or short coming observed shall be brought to the notice of the Management Committee / Audit Committee.

The compliance function shall also provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

7. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the Customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the Customer. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk Customers have to be subjected to intensified monitoring.

The Company shall put in place an appropriate system / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of Customers.

The Company should ensure that a record of transactions with Customers is preserved and maintained as required in terms of Section 12 of the PMLA and Para 46 of the RBI Directions. It may also be ensured that transactions of suspicious nature and/or any other type of transaction notified under the PMLA, is reported to the appropriate law enforcement authority, in the prescribed form and within the stipulated time frame.

8. Appointment of the Designated Director and the Principal Officer

To ensure effective implementation of this Policy, the Board of Directors shall appoint / designate Managing Director / Whole-Time Director of the Company, as the Designated Director who shall be responsible for ensuring overall compliance as required under this Policy, the RBI Directions, PMLA and the Rules made thereunder and the Principal Officer, who shall be responsible for furnishing / reporting all transactions and sharing of information as required under the law to the Director, Foreign Intelligence Unit – India (FIU-IND) and other enforcement agencies. In no case the Principal Officer shall be appointed as the Designated Director.

The name of the Designated Director and the Principal Officer so designated and other information shall be intimated to the Director, FIU-IND and to RBI / National Housing Bank, as the case maybe.

9. Reporting to Financial Intelligence Unit - India

Information / reporting with respect to Cash Transactions & Suspicious Transactions as required in terms of the PMLA and the Rules made thereunder shall be furnished to the Director, FIU-IND, in the prescribed formats and within prescribed time frame.

10. Combating Financing of Terrorism

The Company shall ensure that in terms of the Unlawful Activities (Prevention) Act, 1967 (UAPA), the name of the Customer does not appear 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.

Details of accounts resembling any of the individuals / entities in the lists shall be reported to the Director, FIU-IND and shall be advised to the Ministry of Home Affairs.

The Company shall consider the FATF Statements circulated by the Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations. Special attention shall be given to business relationships and transactions with individuals / entities from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

11. Reporting Requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

The Designated Director and the Principal Officer shall ensure compliance with the requirements under the FATCA and CRS.

The Company shall register itself as Reporting Financial Institution and shall submit online reports with the Income Tax Department.

12. Employee Training

The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new Customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

13. Customer Education

The Company shall prepare specific literature/pamphlets etc. so as to educate the Customer of the objectives

of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joiners on the elements of KYC through various training programmes and e-mails.

14. Introduction of New Technologies

The Company shall pay special attention to any money laundering and financing of terrorism threats that may arise from new or developing technologies in the implementation of the Policy and shall ensure that appropriate KYC procedures issued from time to time are duly applied before introducing new products / services / technologies.

15. Record Retention

The Company has in place a policy on record retention duly approved by the Board and as may be amended from time to time.

The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

16. Review of Policy

This Policy shall be reviewed as and when considered necessary by the Board.

Customer Identification

Customer Type and features to be verified	Documents / Information
<p>Individuals</p> <ul style="list-style-type: none"> - Legal name / any other name used - Correct Permanent and Current Address - Nature of business & financial status 	<ul style="list-style-type: none"> - A certified copy of the following documents to be obtained for verifying identity and address: <ul style="list-style-type: none"> • PAN or Form 60 (Mandatory) • proof of possession of Aadhaar Number • passport • driving licence • Voter's Identity Card issued by the Election Commission of India • job card issued by NREGA duly signed by an officer of the State Government • Letter issued by the National Population Register containing details of name, address • The documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India – only for Foreign Nationals as proof of address - In case the abovementioned documents do not contain the current address, pending updation of current address on such documents, a certified copy of any of the following documents to be obtained, which will be valid only for 3 months: <ul style="list-style-type: none"> • utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); • property or municipal tax receipt; • pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; • letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation - Documents with respect to nature of business and financial status as may prescribed by Management Committee from time to time - Recent Photograph - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time <p>In this Annexure obtaining a certified copy by the Company shall mean comparing the copy of the document so produced by the Customer with the original and recording the same on the copy by person authorised by the Company.</p> <p>Where a person submits a proof of possession of Aadhaar Number</p>

Customer Type and features to be verified	Documents / Information
	<p>containing his Aadhaar Number for the purpose of proof of identity and / or address, it shall be ensured such person redacts or blacks-out his Aadhaar Number through appropriate means.</p> <p>The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder and the RBI Directions.</p>
<p>Sole Proprietorship</p> <ul style="list-style-type: none"> - Correct address / place of business of the proprietor and firm - Business / activity of the firm - Contact Point Verification 	<p>Documents to be obtained from Proprietor:</p> <ul style="list-style-type: none"> - Documents to be obtained from “Individual Customers” <p>Documents to be obtained from the Proprietary Firm:</p> <ul style="list-style-type: none"> - Any two of the following documents as proof of business / activity in name of proprietary firm: <ul style="list-style-type: none"> • Registration certificate including Udyam Registration Certificate (URC) issued by the Government • Certificate/licence issued by the municipal authorities under Shop and Establishment Act. • Sales and income tax returns. • CST/VAT/GST certificate (provisional / final). • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. • IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute • Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. • Utility bills such as electricity, water, and landline telephone bills <p>Where the Company is satisfied that it is not possible to furnish two such documents, the Company may accept only one of those documents as proof of business/activity; provided contact point verification has been undertaken and such other information and clarification has been collected which would be required to establish the existence of such firm, and the Company shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.</p> <ul style="list-style-type: none"> - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time
<p>Partnership</p> <ul style="list-style-type: none"> - Legal name - Address 	<p>Documents to be obtained from beneficial owner, managers, officers or employees holding an attorney to transact on behalf of the Partnership Firm:</p>

Customer Type and features to be verified	Documents / Information
<ul style="list-style-type: none"> - Names of all partners and their addresses - Ultimate Beneficial Owners - Telephone numbers of the firm and partners 	<ul style="list-style-type: none"> - Please refer to documents to be obtained from “Individual Customers” <p>Documents to be obtained from the Partnership Firm:</p> <ul style="list-style-type: none"> - Registration certificate - Partnership deed - Permanent Account Number of the Partnership Firm - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - the name of all the partners address of the registered office, and the principal place of its business, if it is different - Such other documents as may be prescribed from time to time
<p>Trust</p> <ul style="list-style-type: none"> - Names of trustees, settlers, beneficiaries - Telephone/fax numbers 	<p>Documents to be obtained from beneficial owner, managers, trustee, officers or employees holding an attorney to transact on behalf of the Trust:</p> <ul style="list-style-type: none"> - Please refer to documents to be obtained from “Individual Customers” <p>Documents to be obtained from the Trust:</p> <ul style="list-style-type: none"> - Registration certificate - Trust Deed - Permanent Account Number or Form No.60 of the Trust - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - the address of the registered office of the trust - Such other documents as may be prescribed from time to time
<p>Unincorporated Association or Body of Individuals (includes unregistered trust / partnership firms and societies)</p> <ul style="list-style-type: none"> - Business / activity - Legal existence - Principal place of business - Ultimate Beneficial Owner - Contact Point Verification 	<p>Documents to be obtained from beneficial owner, managers, officers or employees holding an attorney to transact on behalf of the unincorporated association / body of individuals:</p> <ul style="list-style-type: none"> - Please refer to documents to be obtained from “Individual Customers” <p>Documents to be obtained from Unincorporated Association or Body of Individuals:</p> <ul style="list-style-type: none"> - Resolution of the managing body of such association or body of individuals - Permanent Account Number or Form No. 60 of the Unincorporated Association or a Body of Individuals - Power of attorney granted to transact on its behalf - Documents to collectively establish the Legal existence of the association / body of individuals - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time
<p>Companies</p> <ul style="list-style-type: none"> - Name of the company, directors & promoters - Principal place of business - Ultimate Beneficial Owners - Mailing address of the company 	<p>Documents to be obtained from beneficial owner, managers, officers or employees holding an attorney to transact on behalf of the company:</p> <ul style="list-style-type: none"> - Please refer to documents to be obtained from “Individual Customers” <p>Documents to be obtained from companies:</p> <ul style="list-style-type: none"> - Certificate of incorporation; - Memorandum and Articles of Association;

Customer Type and features to be verified	Documents / Information
<ul style="list-style-type: none"> - Telephone/Fax Number 	<ul style="list-style-type: none"> - Permanent Account Number of the company - A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on behalf of the company; - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - the names of the relevant persons holding senior management position; - the registered office and the principal place of its business, if it is different; - Such other documents as may be prescribed from time to time
<p>Juridical persons not specifically covered in the earlier section, such as Government or its Departments, societies, universities and local bodies like village panchayats</p> <ul style="list-style-type: none"> - Legal existence - Contact Point Verification - Identity of Person purporting to act on behalf on its behalf 	<p>A copy of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> - Document showing name of the person authorised to act on behalf of the entity; - For documents to be obtained from person holding attorney to transact on behalf of the entity - Please refer to documents to be obtained from “Individual Customers” - Such documents as may be required by the Company to establish the legal existence of such an entity. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time

In terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, equivalent e-document of the abovementioned documents can be obtained for the purpose of KYC in compliance with the said rules.

The Management Committee shall frame rules for conduct of Digital KYC in terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

Annexure – II

Indicative Risk Categorisation of Customers

Customers whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorised as low risk. Customers that are likely to pose a higher than average risk of money-laundering should be categorised as Medium or High Risk Customers, depending on customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc.

Low Risk (Grade A)
<i>Illustrative examples of Low Risk Customers:</i>
Listed companies or their majority owned subsidiaries in India
Entities that are regulated by any Indian financial sector regulator like SEBI, RBI or IRDA.
Government departments & Government owned companies, regulators, statutory bodies and juridical bodies created under a law in force in India
Individuals / entities like salaried or self-employed individuals, professionals, proprietary firms, partnership firms, hindu undivided family, trusts, private / public limited companies, with clear sources of funds verifiable through documents like IT Returns, statutory filings, documents registered / filed with statutory authorities, etc.
Medium Risk (Grade B)
<i>Illustrative examples of Medium Risk Customers:</i>
Entities belonging to business groups where at least two major entities are companies listed in India
Entities belonging to business group where at least one major entity is regulated by an Indian financial sector regulator like SEBI, RBI or IRDA. However, if the regulated entity is a stock broker or an insurance broker, this sub-rule cannot be applied
Entities whose loan has been purchased from, or is assigned to us by a listed NBFC
Entities that have a credit rating of AA or higher from 2 or more SEBI approved Indian rating agencies
Entities like proprietary firms, partnership firms, hindu undivided family, trusts, private / public limited companies, with clear sources of funds verifiable through documents like IT Returns, statutory filings, documents registered / filed with statutory authorities, etc., with transaction size of more than INR 50 crore.
High Risk (Grade C)
<i>Illustrative examples of High Risk Customers:</i>
Entities that cannot be covered under KYC Grade A or B, as per specified criteria.
Non-residents / Foreign Nationals
High Net Worth Individuals i.e. individuals with net worth of more than INR 10 crore
Trusts, charities, NGOs and other organizations receiving donations
Firms with 'sleeping partners'
Entities / Individuals engaged in / deriving income from activities related to Real Estate sector.
Politically exposed or connected Customer / Beneficial Owner
Multi-level Marketing Companies
Customers in jurisdictions that do not or insufficiently apply the FATF Recommendations
Customers with dubious reputation as per public information

- The Grade assigned to a customer, must be clearly indicated in the relevant Credit Appraisal Memo; and the intensity of due diligence for each customer will depend on its risk category.
- KYC Grading guidelines mentioned above are indicative. In case of ambiguity on classification, the next higher KYC Grade must be applied. For instance a real estate company that is listed on NSE would be covered under KYC Grade A, by virtue of being listed. However since its primary business is Real Estate, KYC Grade C would be applicable. In view of the ambiguity because one of either of these KYC Grades could be applied, KYC Grade C is to be applied.