Clix Housing Finance Limited (Formerly known as Clix Housing Finance Private Limited)

KNOW YOUR CUSTOMER (KYC) GUIDELINES & ANTI-MONEY LAUNDERING STANDARDS (AML) POLICY

Governing Guidelines	Reserve Bank of India (RBI) Master Direction-Know Your Customer (KYC) Direction, 2016
Owner	Compliance
Document type	Internal
Original Issue Date	February 15, 2018
Version	1.0 of 2021
Last revision approved by the Board	June 30, 2020
Current revision date and Board approval	June 29, 2021

Contents

1. Glossary

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PMLA	Prevention of Money-Laundering Act
PEP	Politically Exposed Person
KYC	Know Your Customer
AML	Anti-Money Laundering
NBFC	Non-Banking Financial Companies
CTR	Cash Transaction Report
STR	Suspicious Transaction Report
FIU-IND	Financial Intelligence Unit-India
CIBIL	Credit Information Bureau (India) Limited
UIDAI	Unique Identification Authority of India
OVD	Officially Valid Document
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest
NRI	Non Resident Indian
PIO	Person of Indian Origin

2. Applicability

The Know Your Customer, Anti-Money Laundering and Counter-Terrorism Financing Policy (the "Policy") applies to the Company, its subsidiaries and affiliates. The Policy also applies to any third parties relied upon or used by the Company to perform any of the requirements of its Anti-Money Laundering ("AML") Program.

This Policy is consistent with and effectively implements the Reserve Bank of India's Master Directions – Know Your Customer (KYC) Direction, 2016 (updated as on May 10, 2021). Non-Compliance with the Policy can result in serious consequence.

This Policy requires the Company and each Employee to:

- Protect the Company from being used for money laundering or funding terrorist activities;
- Comply with the letter and the spirit of applicable AML/CTF Laws, and the Company's AML Program and procedures;
- Be alert to and escalate suspicious activity; and
- Cooperate with AML-related law enforcement and regulatory agencies to the extent permitted under applicable laws.

3. Policy Review

The Policy shall be reviewed periodically by the Board of Directors of the Company, the AML Leader/ the Principal Officer and, more frequently, if there changes are required by the applicable rules and regulations.

4. Policy Approval

The Policy and any significant changes therein shall be approved by the Board of Directors of Clix. Prior to approval by the Board of Directors, the Policy and any significant changes are also be reviewed and approved by the Company's AML Leader/ Principal Officer.

5. Background

To address money laundering, the Government of India and other countries around the world have made money laundering a crime and imposed regulatory requirements on banks, financial institutions and other businesses to prevent and detect money laundering. In India and in many other countries, it is a crime to engage in a transaction with knowledge that the funds involved in the transactions are from illegal activity. Knowledge includes the concept of willful blindness – failure to make appropriate inquiries when faced with suspicion of wrongdoing.

To prevent money-laundering in India and to provide for confiscation of property derived from, or involved in, money-laundering and related matters, the Parliament of India enacted the Prevention of Money Laundering Act, 2002 (PMLA), as amended from time to time, which came into effect from 1st July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and the Government of India.

The PMLA and rules notified thereunder impose obligation on banking companies, financial institutions (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediaries which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) to verify identity of clients, maintain records and furnish information to Financial Intelligence Unit- India (FIU-IND). The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

Reserve Bank of India has been issuing guidelines in regards to The 'Know Your Customer' guidelines. They were issued in February 2005 revisiting the earlier guidelines issued in January 2004 and later revised from time to time.

Know Your Customer (KYC) standards to be followed by Non-Banking Financial Companies (NBFCs) and measures to be taken in regard to Anti Money Laundering (AML) and Combating Financial Terrorism (CFT) incorporate the-

- Obligations cast on banks/ financial companies under the Prevention of Money Laundering Act (PMLA), 2002
- Recommendations made by the Financial Action Task Force (FATF) on AML standards and CFT
- Paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision

All NBFCs have, therefore, been advised to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of their Board.

The Company is committed to preventing its products and services from being used for money laundering, terrorist financing, and other criminal purposes. The Company is required to fully comply with the local applicable AML/CTF Laws. The term "AML Program" in this document refers to a program that is reasonably designed to (a) comply with applicable AML/CTF Laws and (b) prevent and detect money laundering and terrorist financing activity.

As a well-regulated entity, the Company maintains AML Program that governs its business. The Policy establishes minimum standards and principles and outlines the support and oversight of the Company's AML program.

The Company's AML Program is risk-based and designed to address the AML/CTF risk posed by its business, customers, products and services in various geographic locations and markets. The Company's AML Program is designed to comply with applicable AML/CTF Laws and to prevent the Company's from facilitating money laundering, terrorism, and terrorist financing activity and to mitigate the risk of criminal, civil, administrative, and regulatory liability for violations of applicable AML/CTF Laws, regulatory sanctions, material financial loss, and damage to reputation that the Company may suffer as a result of failing to comply with AML/CTF Laws.

6. Policy Standard and AML Program Structure

The Company has an AML Program, including procedures and internal controls, which is customized to address the money laundering and terrorist financing risks in the Company. The AML Program and procedures of the Company are approved by the Board of the Company.

7. The Company, its Business Segments and Employees Responsibilities

The Board is responsible for overseeing the structure and management of the Company's AML Program, setting an appropriate culture of AML compliance across the Company, reviewing and approving this Policy periodically and providing oversight by reviewing, at such intervals as and when deemed necessary, the operation of the Company's 's AML Program.

The Company's AML Leader/ Principal Officer/Designated Director is responsible for, among others, creating, implementing and maintaining the strategy for, and overseeing and monitoring compliance with the Company's AML Program. The role of the Company's AML Leader/ Principal Officer/Designated Director includes reporting on required matters to the Regulatory Authorities including Financial Intelligence Unit, the Board of Directors, the Chief Compliance Officer / AML Leader. To be able to exercise these responsibilities, the AML Leader/ Principal Officer/Designated Director must receive prompt and accurate information from various functions of the Company.

8. Anti-Money Laundering Program

The Company's AML Program shall include the following elements, which are further detailed in subsequent provisions of this Policy:

- A senior official of the Company shall be designated as the AML Leader/ the Principal Officer of the Company. The AML Leader/ the Principal Officer shall be responsible for overseeing and managing the AML Program. The AML Leader/ the Principal Officer shall be responsible for the day-to-day functioning of the Company's AML Program and must have the knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business. The designated person will also have oversight responsibility for compliance with the Government Recommended Watchlist Guidelines
- Risk assessments of the AML Program.
- Inclusion of an AML risk assessment component in the Company's New Product Introduction ("NPI") process that reviews proposed new or revised products/services and, if appropriate, incorporates elements of product design, distribution or other controls to mitigate AML risk.
- Clearly defined and documented acceptable forms and limitations or prohibitions on payments that may be associated with money laundering, including development of controls that ensure compliance by Employees or third parties that accept or process payments for the Company
- Written risk-based AML procedures that set forth adherence to applicable AML laws and regulations and the requirements set forth in this Policy, including:
- Reasonable Know Your Customer ("KYC") procedures that are consistent with the requirements of this Policy and that are tailored to the Company's money laundering risk, including Customer Identification

Program ("CIP"); Customer Due Diligence ("CDD"); Simplified Due Diligence ('SDD") and Enhanced Due Diligence ("EDD") procedures.

- Procedures for filing reports and/or maintaining records of large currency/ cash transactions and cross-border movements of currency and negotiable instruments as required by applicable law or regulation.
- Procedures for Employees to refer internally potentially suspicious activity and for monitoring customers and their transactions to detect suspicious activity.
- Procedures for investigating and escalating suspicious matters internally as required, including a decision-making process to determine whether or not to file a Suspicious Transaction Report ("STR") and/or take other appropriate action, including terminating a customer relationship.
- Procedures for reporting of suspicious activity to government authorities where required or, in appropriate cases, permitted in accordance with applicable laws and regulations.
- AML training, pursuant to a training plan, for all appropriate Employees, the frequency and content of which is based upon possible exposure to money laundering risk and the extent of AML duties performed by the Employee.
- Compliance testing and monitoring of the Company's adherence to its AML Program as further described in this Policy.
- Periodic independent testing and auditing of the AML Program appropriate to the level of money laundering risk of the Company.

9. Money Laundering Risk Assessment

The development and implementation of an effective AML Program at every functional level must be based on a risk assessment. For this reason, the Company is required to conduct formal AML/CTF risk assessments of its business, customers, products and services, and geographic locations and markets, in accordance with a standard risk assessment methodology developed by the company, or basis any best practices that are being followed by the industry or industry leaders.

The AML leader/ the Principal Officer must determine the AML vulnerabilities of its products/services, the AML risks associated with the geographies in which it operates, and the AML risks of the customers with which it deals. The AML leader/ the Principal Officer must also assess the effectiveness of its controls to manage and mitigate the AML risks. The selection of risk categories and weights given to risk categories in money laundering risk assessment varies depending on the circumstances. In order to provide a framework for identifying AML risks and for comparing the degree of potential money laundering risk across the functions, The AML leader/ the Principal Officer conducts money laundering risk assessment.

Any new product or sales activity or new line of business must undergo an AML risk assessment as described in this Section. In addition, money laundering risk assessment component must be included in the Company's NPI process that reviews the proposed new or revised product and, if appropriate, incorporates elements of product design, distribution or other controls to mitigate AML risk. The NPI process must include procedures for managing and mitigating any new or increased AML risk created by the launch of the new product or significant changes to existing products.

9A Money Laundering and Terrorist Financing Risk Assessment:

(a) The Company carries out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc
The assessment process considers all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to is applied. While preparing the internal risk

assessment, The Company takes cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

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

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

The Company shall apply the Risk Based Approach (RBA) for mitigation and management of the identified risk should have Board Approved Policies, Controls and procedures in this regard. Further, the company shall monitor the implementation of the Controls and enhance them if necessary.

10. Definitions

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

i. "Aadhaar number"

shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. "Act" and "Rules"

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

iii. "Authentication"

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

iv. Beneficial Owner (BO)

a. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
   Explanation- For the purpose of this sub-clause-
   - "Controlling Ownership interest," means ownership of/entitlement to more than 25 percent of the shares or capital or the profits of the company.
   - "Control "shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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

c. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
   Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. "Certified Copy"

Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.

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

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

vi. "Central KYC Records Registry" (CKYCR)

Means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vii. "Common Reporting Standards" (CRS)

Means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

viii. "Customer"

Means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

ix. "Customer Due Diligence (CDD)"

Means identifying and verifying the customer and the beneficial owner.

x. Customer identification"

Means undertaking the process of CDD.

xi. "Designated Director"

Means a person designated by Clix to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include a whole-time Director, duly authorized by the Board of Directors.

Explanation - For the purpose of this clause, the terms "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

xii. "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 Clix as per the provisions contained in the Act.

xiii. "Digital Signature"

shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

xiv. "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.

xv. "FATCA"

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

xvi. **"IGA"**

Means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

xvii. "Know Your Client (KYC) Identifier"

Means the unique number or code assigned to a customer by the Central KYC Records Registry.

xviii. "KYC Templates"

Means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

xix. "Non-face-to-face customers"

Means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

xx. "Non-profit organizations" (NPO)

Means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xxi. "Officially Valid Document" (OVD)

Means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
   i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
   ii. property or Municipal tax receipt;
   iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
   iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

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

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

xxii. "Offline verification"

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

xxiii. "On-going Due Diligence"

Means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

xxiv. "Periodic Updation"

Means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xxv. "Person"

It has the same meaning assigned in the Act and includes:

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

xxvi. "Politically Exposed Persons" (PEPs)

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/ Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

xxvii. "Principal Officer"

Means an officer nominated by Clix, responsible for furnishing information as per rule 8 of the Rules.

xxviii. "Regulated Entities" (REs)

Means as defined in RBI Master Directions on KYC – last updated on January 09, 2020.

xxix. "Suspicious transaction"

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

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

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

xxx. "Video based Customer Identification Process (V-CIP)"

Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of Clix by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP.

11. This policy includes following four key elements:

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

12. Designated Director:

a) A "Designated Director" means a person designated by Clix to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.
b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
c) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

13. Principal Officer:

a) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

14. Compliance of KYC policy

(a) Clix shall ensure compliance with KYC Policy through:

(i) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements.
(iv) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
(v) Submission of quarterly audit notes and compliance to the Audit Committee.

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

15. Customer Acceptance Policy

Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, Clix shall ensure that:

a. No account is opened in anonymous or fictitious/benami name.
b. No account is opened where Clix is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
c. No transaction or account-based relationship is undertaken without following the CDD procedure.
d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
e. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
f. Clix shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a Clix desires to open another account with them, there shall be no need for a fresh CDD exercise.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
k. Where an equivalent e-document is obtained from the customer, Clix verifies the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

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

16. Risk Management

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

a. Customers are categorised as low, medium and high risk category, based on the assessment and risk perception of Clix.
b. Risk categorisation is undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
   Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.
   Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

17. Customer Identification Procedure (CIP)

Clix shall undertake identification of customers in the following cases:

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

18. Rely on Third Party Customer Due Diligence

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

a. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
b. Adequate steps are taken by Clix to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements is made available from the third party upon request without delay.
c. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
d. The third party shall not be based in a country or jurisdiction assessed as high risk.
e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

Customer Due Diligence (CDD) Procedure

19. Customer Due Diligence (CDD) Procedure in case of Individuals

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

(a) the Aadhaar number where,

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

Note: Clix is not yet notified under section 11A of PML Act. Till the time of such notification, this authentication cannot be performed.

II. he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

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

(c) 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 RE:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank or to a Clix notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or Clix shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India (this is subject to approval by UIDAI). Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Company.

ii) Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, Clix shall carry out offline verification.

iii) An equivalent e-document of any OVD, Clix shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

iv)Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, Clix shall carry out verification through digital KYC as specified under Section 52.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Clix 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.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, REs shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Clix and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Clix ensures to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by Clix and shall be available for supervisory review.

Explanation 1: RE ensures, 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 where the authentication of Aadhaar number is not required as per proviso (i) above.

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.

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

a) There is a specific consent from the customer for authentication through OTP.
b) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
c) As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

d) Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 19 or as per Section 21 (V-CIP) is carried out. If Aadhaar details are used under Section 21, the process shall be followed in its entirety including fresh Aadhaar OTP authenticationIf the CDD procedure as mentioned above is not completed within a year, in respect of borrowal accounts, no further debits shall be allowed.

e) A declaration is obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, Clix shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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

21.V-CIP

Clix may undertake V-CIP to carry out:

i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
Provided that in case of CDD of a proprietorship firm, Clix shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 24, apart from undertaking CDD of the proprietor.

ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 20.

iii. Updation/Periodic updation of KYC for eligible customers.

Clix opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

i. Clix should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of Clix and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii. Clix shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv. The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v. 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 Clix. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-event under extant regulatory guidelines.

vii. 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 suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii. The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, 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.

(b) V-CIP Procedure

i. Clix shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of Clix specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii. If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

iii. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

iv. Any prompting, observed at end of customer shall lead to rejection of the account opening process.

v. 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 work flow.

vi. The authorised official of the Company 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) OTP based Aadhaar e-KYC authentication
b) Offline Verification of Aadhaar for identification
c) KYC records downloaded from CKYCR, in accordance with Section 40, using the KYC identifier provided by the customer
d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Clix shall ensure to redact or blackout the Aadhaar number in terms of Section 19.
In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.
Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Clix shall ensure that the video process of the V-CIP is undertaken within three 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, Clix shall ensure that no incremental risk is added due to this.

vii. 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.

viii. Clix shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

ix. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
x. The authorised official of Clix 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.
xi. 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.
xii. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by Clix.

(c) V-CIP Records and Data Management

i. The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Clix shall ensure that the video recording is 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 this MD, shall also be applicable for V-CIP.
ii. ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

22. Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs):

In case a person who desires to open an account is not able to produce documents, as specified in Section 19, Clix may at their discretion open accounts subject to the following conditions:

a. Clix shall obtain a self-attested photograph from the customer.
b. The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
c. The account shall remain operational initially for a period of twelve months, within which CDD as per Section 19 shall be carried out.
d. Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
e. The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
f. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.
g. The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

23. KYC verification once done by one branch/office of the Clix

shall be valid for transfer of the account to any other branch/office of Clix, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

24. CDD Measures for Sole Proprietary firms

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

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

a. Registration certificate
b. Certificate/ licence issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. CST/VAT/ GST certificate (provisional/final).

e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License /certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. 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.
h. Utility bills such as electricity, water, landline telephone bills, etc.

In cases where the Company is satisfied that it is not possible to furnish two such documents, Clix may, at its discretion, accept only one of those documents as proof of business/activity.

Provided the Company undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

25. CDD Measures for Legal Entities

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

a. Certificate of incorporation
b. Memorandum and Articles of Association
c. Permanent Account Number of the company
d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
e. Documents, as specified in Section 19, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

26. For opening an account of a partnership firm,

The certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate
b. Partnership deed
c. Permanent Account Number of the partnership firm
d. Documents, as specified in Section 19, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

27. For opening an account of a trust,

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate
b. Trust deed
c. Permanent Account Number or Form No.60 of the trust
d. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

28. For opening an account of an unincorporated association or a body of individuals,

Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Resolution of the managing body of such association or body of individuals

b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
c. Power of attorney granted to transact on its behalf
d. Documents, as specified in Section 19, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
e. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

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

29. For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats,

Certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

a. Document showing name of the person authorised to act on behalf of the entity;
b. Documents, as specified in Section 19, of the person holding an attorney to transact on its behalf and
c. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

30. Identification of Beneficial Owner

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

a. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
b. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

31. On-going Due Diligence

Clix shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.
Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

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

The extent of monitoring is aligned with the risk category of the customer.
Explanation: High risk accounts are subjected to more intensified monitoring.

A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and enhanced due diligence measures shall also be applied.

The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies are closely monitored.

32. Periodic Updation (KYC Refresh)

Clix shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

a) Individual Customers:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with Clix, customer's mobile number registered with the Clix, digital channels (such as mobile application of Clix), letter etc.

ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with Clix, customer's mobile number registered with the Clix, digital channels (such as mobile application of Clix), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, Clix, at its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 10(xxi), for the purpose of proof of address, declared by the customer at the time of periodic updation.

b) Customers other than individuals:

i. **No change in KYC information:** In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with Clix, digital channels (such as mobile application of Clix), letter from an official authorized by the LE in this regard, board resolution etc. Further, Clix shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. **Change in KYC information:** In case of change in KYC information, Clix shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

c) Additional measures: In addition to the above, Clix shall ensure that,

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

B. Customer's PAN details, if available with Clix, is verified from the database of the issuing authority at the time of periodic updation of KYC.

C. 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, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of Clix and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

D. Clix shall ensure that internal processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

Enhanced and Simplified Due Diligence Procedure

33. Enhanced Due Diligence

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

B. Accounts of Politically Exposed Persons (PEPs)

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

a. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
b. the identity of the person shall have been verified before accepting the PEP as a customer;
c. the decision to open an account for a PEP is taken at a senior level in accordance with the REs' Customer Acceptance Policy;
d. all such accounts are subjected to enhanced monitoring on an on-going basis;
e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
f. the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

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

C. Client accounts opened by professional intermediaries:

Clix shall ensure while opening client accounts through professional intermediaries, that:

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

34. Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Clix shall,

(a) Maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;

(b) Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
(c) Make available the identification records and transaction data to the competent authorities upon request;
(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

I. the nature of the transactions;
II. the amount of the transaction and the currency in which it was denominated;
III. the date on which the transaction was conducted; and
IV. the parties to the transaction.

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

35. Reporting Requirements to Financial Intelligence Unit - India

a) Clix shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.
Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.
b) The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those REs, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.
c) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. REs shall not put any restriction on operations in the accounts where an STR has been filed. REs shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
d) Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

36. Requirements/obligations under International Agreements Communications from International Agencies

a) Clix shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, Company 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.

b) Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021 (Annex II of this RBI Master Direction on KYC)..

c) In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

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

The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of this RBI Master Direction on KYC). (Annex II of this Master Direction) are strictly followed and meticulous compliance with the Order issued by the Government is ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

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

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

Explanation: The process referred to in Section 36 a & b do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

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

39. Other Instructions

Secrecy Obligations and Sharing of Information:

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

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

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

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

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

(e) Clix shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

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

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

b) In terms of provision of Rule 9(1A) of PML Rules, Clix shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

d) Clix shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

e) Regulated Entities other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

f) Clix shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

g) Once KYC Identifier is generated by CKYCR, Clix shall ensure that the same is communicated to the individual/LE as the case may be.

h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Clix shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 32 of this policy, or earlier, when the updated KYC information is obtained/received from the customer.

i) Clix shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

j) Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to Clix, with an explicit consent to download records from CKYCR, then Clix 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 –

a. there is a change in the information of the customer as existing in the records of CKYCR;
b. the current address of the customer is required to be verified;
c. Clix considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

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

Under FATCA and CRS, Clix shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are 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: REs shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.
(c) Clix is developing Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
(d) It has a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
(e) Clix constitutes a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
(f) Clix ensures 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. It may take note of the following:

I. updated **Guidance Note** on FATCA and CRS
II. a **press release** on 'Closure of Financial Accounts' under Rule 114H (8).

42. Period for presenting payment instruments

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

43. Operation of Accounts & Money Mules

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

44. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent are not collected. Banks shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

45. UCIC

a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by Clix.
b) The Company shall, at its option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

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

Adequate attention shall be paid by Clix to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it is ensured that appropriate KYC procedures issued

from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

47. Issue and Payment of Demand Drafts, etc.,

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

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

48. Quoting of PAN

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

49.Selling Third party products

REs acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects:

a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 17(e) of this Policy.
b) transaction details of sale of third party products and related records shall be maintained as prescribed in Section 34 of this policy.
c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
    a. transactions involving rupees fifty thousand and above shall be undertaken only by:
    b. debit to customers' account or against cheques; and
d) obtaining and verifying the PAN given by the account-based as well as walk-in customers.
e) Instruction at 'd' above shall also apply to sale of the Company' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

50.Hiring of Employees and Employee training

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

51. Adherence to Know Your Customer (KYC) guidelines by NBFCs and persons authorised by NBFCs including brokers/agents etc.

a. Persons authorised by NBFCs for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to NBFCs.
b. All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs including brokers/agents etc. who are operating on their behalf.
c. The books of accounts of persons authorised by NBFCs including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

52. Digital KYC Process

A. Clix may develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of Clix.
B. The access of the Application shall be controlled by Clix and it is being ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Clix to its authorized officials.
C. The customer, for the purpose of KYC, shall visit the location of the authorized official of Clix or vice-versa. The original OVD shall be in possession of the customer.
D. Clix must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
E. The Application of Clix shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with Clix shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with Clix. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of Clix, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of Clix shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of Clix who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

53. Revision History:

Dates	**Rationale**
June xx, 2021	Changes done w.r.t. V-CIP and Periodic updation etc. as per the amendments to Master Direction on Know Your Customer, 2016, updated on May 10, 2021.
March 09, 2021	Amended Para 40 w.r.t CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) as per RBI Master Direction on Know Your Customer, 2016
June 30, 2020	Para 9A has been inserted in the policy as per the new section 5A of the RBI Master Direction on Know Your Customer, 2016, updated on 20 April 2020
February 14, 2020	This document replaces the earlier version of AML/ KYC Policy and in line with the RBI Master KYC Direction last updated on January 09, 2020.
April 14, 2019	Changes done as per the amended Master Directions on Know Your Customer
February 15, 2018	Original Issue Date

Annexure-I

A. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER/ PROJECT/ CORPORATE CLIENTS:

1. Builder approaching the Company for a small loan compared to the total cost of the project;
2. Builder is unable to explain the sources of funding for the project;
3. Approvals/ sanctions from various authorities are proved to be fake or if it appears that client does not wish to obtain necessary governmental approvals/ filings, etc.;
4. Management appears to be acting according to instructions of unknown or inappropriate person(s).
5. Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
6. Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.
7. Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/ corporate seat or other complex group structures).
8. Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.

B. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO INDIVIDUALS:

1. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
2. Unnecessarily complex client structure.
3. Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
4. Customer is reluctant to provide information, data, documents;
5. Submission of false documents, data, purpose of loan, details of accounts;
6. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
7. Reluctant to meet in person, represents through a third party/ Power of Attorney holder without sufficient reasons;
8. Approaches a branch/ office of a Company, which is away from the customer's residential or business address provided in the loan application, when there is COMPANY branch/ office nearer to the given address;
9. Unable to explain or satisfy the numerous transfers in account/ multiple accounts;
10. Initial contribution made through unrelated third party accounts without proper justification;
11. Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount;
12. Suggesting dubious means for the sanction of loan;
13. Where transactions do not make economic sense;
14. Unusual financial transactions with unknown source.

15. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
16. There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
17. Encashment of loan amount by opening a fictitious bank account;
18. Applying for a loan knowing fully well that the property/ dwelling unit to be financed has been funded earlier and that the same is outstanding;
19. Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
20. Multiple funding of the same property/ dwelling unit;
21. Request for payment made in favour of a third party who has no relation to the transaction;
22. Usage of loan amount by the customer in connivance with the vendor/ builder/ developer/ broker/ agent etc. and using the same for a purpose other than what has been stipulated.
23. Multiple funding / financing involving NGO / Charitable Organisation / Small/ Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs)
24. Frequent requests for change of address;
25. Overpayment of instalments with a request to refund the overpaid amount.
26. Investment in real estate at a higher/lower price than expected.
27. Clients incorporated in countries that permit bearer shares

Annexure III

RED FLAGS / PARAMETERS TO IDENTIFY STR

List of RED FLAG INDICATORS (RFI) for STR identification:

In order to facilitate an effective reporting regime of STRs by HFCs, the note identifies a list of RFIs that may be further identified as a Suspicious Transaction and then reported as a STR, upon due verification.

The RFIs are identified as situations that may be encountered by HFCs in particular and are categorized under the following broad categories:

a. Customer Centric;
b. Transaction / Loan Account Centric;
c. Property / Property document Centric; and
d. Cases (falling under a, b & c above) that would require auto reporting
e. List of RFIs pertaining to builder/project loans

As such the suggested RFIs are essentially situations that would require further analysis as they have the potential of being a STR. The Principal Officers are expected to sensitize the respective HFCs of the RFIs and would there be adequate justification, the RFIs may then be reported as STRs to the Principal Officer for further reporting to the FIU. Mere sighting of the enumerated situations is not expected to be reported as a STR on an "as is" basis as the same is in the nature of possible trigger of reporting as a STR and would be accordingly reported after adequate diligence and with proper justification.

As indicated above, the note also identifies situations that may generate Auto triggers within the system of a HFC which may automatically be referred to the respective Principal Officer for reporting as a STR. There are certain parts (as specifically indicated) that would need to be assessed by each HFC, in lines of its business practices, and determine the point of trigger of the RFI for the said HFC. Upon such identification, all HFCs are expected to approve the RFIs by their Board and incorporate the same as a part of their respective KYC policy.

Thus in order to ensure effective reporting of STRs, the note identifies the following transactions/ situations as RFIs which (upon adequate diligence and justification) may be identified as a Suspicious Transaction and then onward reported as a STR.

Part A: RFIs that are Customer Centric:

Sr. No.	Sub-Category	Types
1.	Identity of Customer	a. Submission of false Identification Documents b. Customer holding multiple PAN c. Identification documents which could not be verified within reasonable time or replaced with another set of Identification documents d. Accounts opened with names very close to other reputed business entities e. Customer uses aliases and a variety of similar but different addresses f. Customer spells his or her name differently from one transaction to another, without justification g. Name of customer indicated differently in different KYC documents enabling creation of multiple customer identities h. A customer/company who is reluctant or refuses to provide complete information, data, documents and to reveal details about its activities or to provide financial statements /Employment related documents / KYC documents i. Doubt over the real beneficiary of the loan account j. The customer is reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons. k. The customer approaches a branch/office of a HFC, which is away from the customer's residential or business address provided in the loan application, when there is HFC branch/office nearer to the given address. l. Changes in mailing address of the Customer that raises suspicion. m. Unusual capital, partnership, management or employment structure of companies compared to other institutions in the same sector or general company structure. n. Current data not updated with relevant regulatory authorities, without justification. o. Existing or new partners/shareholders abstaining from giving information about their personal and commercial background, having indications that they did not have interest, education or experience in the field in which the company operates.

2.	Background of a customer	a. The customer details matched with watch lists (e.g. UN list, Interpol list etc.) b. Notice/Letter from a law enforcement agencies / Regulators/ Other Government Agencies: In case of such notices received, Principal Officer would be informed for further action / advice on the matter. This notice shall be treated as an alert to analyse the transactions in such accounts and if the transactions appear to be suspicious the same would be included in the STR along with the details mentioned in the "Ground of Suspicion". These Accounts are to be reported even if they are closed. c. Adverse Media / Public News: Branches / offices would check for adverse media coverage with the names of the customer. The names of customers that are pointed as suspects or accused in such reports shall be searched and in case of matches the same may be further internally analyzed for reporting purposes. d. Customer shows income from "foreign sources" on loan application without providing proper documentation.

Part B: RFIs that are Transaction / Loan Account Centric:

Sr.	Sub-Category	Types
1.	Multiple Accounts	a. Use of Bank A/c's of Third Parties for payment of EMIs b. Change in the bank account from which PDC/ ECS are issued c. Total amount of payments through DD, Cash and 3rd party Cheques valued at Rs. Two Lakhs EMIs / part payments in last 30 days d. Customer appears to have recently established a series of new relationships with different financial entities.

2.	Nature of Activity in an Account	a. Unusual activity compared with past transactions. b. Encashment of loan amount by opening a fictitious bank account. c. Activity inconsistent with what would be expected from declared business/profile of the customer. d. Part closure to the extent of 25 % or more of the loan amount in one or more occasions within 6 months. e. Loan Accounts with original tenor of more than year are foreclosed within 6 months after disbursal of loan. f. Usage of loan amount by the customer in connivance with the vendor/builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated. g. Overpayment of installments in cash with a request to refund the excess amount. h. Customer conducts transactions at different physical locations in an apparent attempt to avoid detection. i. Customer presents confusing details about the transaction or knows only few details about its purpose. j. Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account. k. Account indicated by customer to receive interest payment against a deposit placed is attached by Government Authorities.

3.	Nature of transactions	a. Unusual or unjustified complexity shown in a Transaction that may normally be done in simpler manner. b. Initial contribution made through unrelated third party accounts without proper justification; c. No economic rationale or bonafide purpose behind the transaction. d. Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount e. Suggesting dubious means for the sanction of loan or placing a deposit. f. PAN not disclosed but multiple deposits raised (across branches to avoid TDS).

4.	Value of transactions	a. Value just under the reporting threshold amount in an apparent attempt to avoid reporting. b. Multiple related cash transactions which are broken to just below the following thresholds: - Rs.50,000/- in a day - Rs.10,00,000/- in a month c. Value inconsistent with the client's apparent financial standing. d. Deposits made in cash amounting to Rs. Two Lakh and above and without details of source.

5.	Transaction amongst family members	Transaction between members of the same family to avail a loan wherein there is no genuine transaction / rationale.

6.	Transaction more than specified percentage of the EMI, paid in cash by a Delinquent Borrower.	Delinquent borrower for more than 6 months repays the loan in cash.

Part C: RFIs that are Property/Property Document Centric:

S. No.	Sub-Category	Types
1.	Cash payment indicated in the Sale Deed/ Agreement	Cash payment shown as consideration paid to the seller for purchase of a property and the source of which cannot be explained or proof not provided by the customer.
2.	Valuation of property	Valuation of property shown considerably lower in the sale deed than the government approved rate / RESIDEX, especially on sale deeds executed within a period of 12 months.
3.	Change in Ownership without rationale	Converting/changing the individual properties in the name of Company/Trust/HUF/Partnership Firm/LLP by executing a sale deed at a low price or by way of any type of agreement, attorney, arrangement (registered or not) and subsequently in quick succession further transaction is shown at a considerably higher amount in favor of third parties.
4.	Refusal to share own Contribution details	Specifically in cases where the source is specified as "Funds from Family" and the customer fails or refuses to divulge any information or proof on where the concerned family member is providing the funds from.
5.	Property repurchased	Customer buys back a property that he or she recently sold without justification

Part D: RFIs that may be considered to be auto generated through a system

S. No.	Scenario	Indicator/ Trigger
1	Foreclosure by a customer in a very short period	Loan Accounts with original tenor of more than 1 year are foreclose within 6 months after disbursal of loan.
2	Frequently change in repayment bank account during currency of account	Change in the bank account from which PDC/ ECS are issued
3	Negative information about customer through external sources/ database or Notice received from any Agency / Regulator/ Other Government Agencies	a. The customer details matched with watch lists (e.g. UN list, Interpol list etc.) b. Notice/Letter from a law enforcement agencies / Regulators/ Other Government Agencies: In case of such notices received, Principal Officer would be informed for further action /advise on the matter. This notice shall be treated as an alert to analyse the transactions in such accounts and if the transactions appear to be suspicious the same would be included in the STR along with the details mentioned in the "Ground of Suspicion". The Accounts are to be reported even if they are closed. c. Adverse Media / Public News: Branches / offices would check for adverse media coverage with the names of the customer. The names of customers that are pointed as suspects or accused in such reports shall be searched and in case of matches the same may be further internally analyzed for reporting purposes.
4	Frequent change of Address without reasonable explanation	Changes in mailing address of the customer in last 6 months that raises suspicion.
5	Account having a large volume of repayments by depositing DD, Cash and 3rd party Cheques	Total amount of payments through DD, Cash and 3rd party Cheques valued at 25% of EMIs / part payments in last 30 days
6	Transaction more than specified percentage of the EMI, paid in cash by a Delinquent Borrower	Delinquent borrower for more than 6 months repays the loan in cash.
7	Cash transactions	Multiple related cash transactions which are broken to just below the following thresholds: (i) Rs.50,000/- in a day
8	Part payments	Part closure to the extent of 25 % or more of the loan amount in one or more occasions within 6 months.
9	Separate bank accounts	Use of Bank A/c's of Third Parties for payment of EMIs

ANNEXURE IV

A. Trigger Review Chart for event based review to periodically update KYC has been embedded below.

		Depth of Review							
		Re-Risk Rate	Refresh CIP	Refresh CDD	Collect or Refresh EDD	Re-Screen for Sanctions	Re-Screen for PEP	Screen or Re-Screen for Negative Media	Review Transaction History
Trigger Event	Name Change	No	Only entity Verification form (e.g., formation doc)	No	No	Yes	Yes	Only if High risk	No
	Address Change - Same jurisdiction	No	Only address	No	No	No	No	No	No
	Address Change - New jurisdiction	Yes	Only address unless CRR changes	Only if CRR changes	Only if CRR changes to High	Yes	Only if CRR changes	Only if CRR changes to High	Only if CRR changes
	Entity Type Change	Yes	Only entity type info and verification form if entity type is indicated in name	Only if CRR changes	Only if CRR changes to High	Only if change in entity type = change in name and/or other KYC changed	Only if CRR changes	Only if CRR changes to High	Only if CRR changes
	Change in Listed or Regulated Status	Yes	Only verification form (e.g., proof of status or formation doc)	Only if CRR changes	Only if CRR changes to High	No	Only if CRR changes	Only if CRR changes to High	Only if CRR changes

	BO Change	Only if screening results warrant (e.g., PEP identified)							
	Control Person Change	Only if Screening results warrant	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Yes, name of new Controllers(s)	Yes, name of new Controllers(s)	Only if CRR changes to High	Only if CRR changes
	Guarantor Change	Only if screening results warrant	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Yes, name of new Guarantor(s)	Yes, name of new Guarantor(s)	Only if CRR changes to High	Only if CRR changes
	Co-Borrower Drawing on Credit	At time of draw	At time of draw	At time of draw	At time of draw	At time of draw	At time of draw	Only if High risk, at time of draw	At time of draw
	New Product	Yes	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Only if CRR changes
	Same Product – New Features	Only if product risk rating changes	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Only if CRR changes	Only if CRR changes	Only if CRR changes to High	Only if CRR changes

	Expansio n of Existing Credit Line	No	No	No	No	No	No	No	Only if TM. not in place
	Same Product - New Deal	No	No	No	No	No	No	No	Possibly
	Business or Industry Change	Yes							
	Law Enforce ment RFI	Yes	Yes	Yes	Yes, if CRR changes to High	Yes	Yes	Yes	Yes
	True Sanction s Hit	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Material & Relevant PEP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	Material Negative News Identifie d	Yes	Only if CRR changes	Only if CRR changes	Yes	Only if CRR changes	Only if CRR changes	Yes	Only if CRR change s
	Transacti onal Monitori ng Event	Yes	If CRR changes or if investigatio n warrants	If CRR changes or if investig ation warrant s	If CRR changes to High or if investig ation warrant s	If CRR changes or if new CIP informat ion, BO or Controll ers are	If CRR changes or if new CIP informat ion, BO or Controll ers are identifie d through investiga tion	Only if CRR changes to High or if new CIP informat ion, BO or Controll ers are identifie	Yes
	SAR Filing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] Based on typical large multi- borrower deals