



**KNOW YOUR CUSTOMER & ANTI MONEY LAUNDERING
POLICY OF
PNB HOUSING FINANCE LIMITED**

Table of Contents

Sections	Page No
1.Preamble.....	4
2.Objective	4
3.Scope.....	4
4.Definitions	4
5.Know Your Customer (KYC) Policy.....	9
6. Money Laundering and Terrorist Financing Risk Assessment.....	9
7.Designated Director & Principal Officer.....	10
8. Compliance of KYC Policy	10
9.Customer Acceptance Policy (CAP)	11
10.Risk Management.....	12
11.Risk Categorization	13
12.Customer Identification Procedure (CIP).....	13
13.Customer Due Diligence (CDD) Procedure.....	14
14.Accounts of Politically Exposed Persons (PEPs):.....	17
15.Ongoing Due Diligence.....	17
16.Periodic Updation	18
17.Monitoring of Transactions and maintenance and preservation of records:	19
18.Furnishing of information to the Director (FIU-IND):	20
19.Reporting Requirement Under Foreign Account Tax Compliance Act (FATCA) And Common ...	21
Reporting Standards (CRS)	21
20.Requirements/obligations under International Agreements	22
21.Other Measures	25
22.Sharing KYC information with Central KYC Records Registry (CKYCR):.....	25
23.Introduction of New Technologies	26
24.Hiring of Employees and Employee training:	26
25.Selling Third party products	27
26. Adherence to Know Your Customer (KYC) guidelines by Company and persons authorised by Company including brokers/agents etc.:	27
27.Enhanced Due Diligence (EDD) Procedure	28
28. Annexures.....	26
29.Abbreviations.....	34

Summary of Version History

Date	Version	Prepared By	Recommended By	Approved by
Jul 19, 2019	V1	-	Audit Committee of Board	Board of Directors
Jan 27, 2021	V2	-	Audit Committee of Board	Board of Directors
Jul 26, 2021	V3	Head Operations & Principal Officer	Audit Committee of Board	Board of Directors
Jul 10, 2023	V4	Head Operations & Principal Officer	Audit Committee of Board	Board of Directors
April 02, 2025	V5	Principal Officer-AML	Audit Committee of Board	Board of Directors
February 27, 2025	V6	Chief Compliance Officer	Audit Committee of Board	Board of Directors

Know Your Customer & Anti Money Laundering Policy of PNB Housing Finance Ltd

1.Preamble

PNB Housing Finance Limited (“the Company”) has adopted “Know Your Customer and Anti Money Laundering” policy for lending/ credit/ operations/ financial dealings, in line with the extant guidelines laid down in the “Master Directions - Know Your Customer (KYC) Direction, 2016” issued and updated from time to time by Reserve Bank of India (“RBI”). The policy is in compliance with the Prevention of Money-Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PMLR) and amendments made there in from time to time.

2.Objective

The objective of the Policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering, terrorist financing, fraud, and other forms of financial crimes. KYC procedures also enable the Company to identify/ know/ understand their customers and their financial dealings better, which in turn help to manage risks prudently.

3.Scope

This Policy applies to Directors, officers, all employees (on-role & off-role), individual agents, DSAs/DMAAs and other contracting parties/vendors of PNB Housing Finance Ltd and its subsidiaries and is to be read in conjunction with related operational guidelines issued from time to time.

4.Definitions

- i. **“Money Laundering”** has the meaning assigned to it under Section 3 of the PMLA 2002, “Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.”
- ii. **“Aadhaar number”**, means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act'.

Explanation 1: In terms of the Aadhaar Act, every resident shall be eligible to obtain an Aadhaar number.

Explanation 2: Aadhaar will be the document for identity and address.

- iii. **“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.

iv. **“Authentication”**, as defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

v. **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 person, has/have a controlling ownership interest or who exercise control through other means.

Explanation-

- *“Controlling ownership interest” means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the Company.*
- *“Control” will include the right to appoint majority of the directors or to control the management or policy decisions including by their virtue of shareholding or management rights or shareholder’s 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 10 per cent of capital or profits of the partnership or who exercises control through other means. (Explanation - For the purpose of this sub-clause, “control” shall include the right to control the management or policy decision)

c) **Where the customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/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 10% 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.

vi. **“Biometric information”**, as defined in the Section 2(g) of the Aadhaar Act, means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by Aadhaar (authentication) regulations.

vii. **“Board”** means Board of Directors of the Company.

viii. **“Cash Transactions”** means "Cash Transactions" as defined under rule 3 of the Rules.

ix. **“Central Identities Data Repository” (CIDR)**, as defined in Section 2(h) of the Aadhaar Act, means a centralized database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic

information and biometric information of such individuals and other information related thereto.

- x. **“Central KYC Records Registry” (CKYCR)** means an entity defined under Rule 2(1)(aa) of the Prevention of Money Laundering Rules 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- xi. **“Company”** means PNB Housing Finance Limited.
- xii. **“Customer”** means a 'person', who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- xiii. **“Customer Due Diligence” (CDD)** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.
- xiv. **“Customer Identification”** means undertaking the process of CDD.
- xv. **“Demographic information”**, as defined in Section 2(k) of the Aadhaar Act, includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.
- xvi. **“Designated Director”** means Managing Director or a whole time Director of the Company duly authorized by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act and the Rules

Explanation. –For the purpose of this clause, the terms "Managing Director" and "Wholetime Director" shall have the meaning assigned to them in the Companies Act, 2013.

- xvii. **“Directors”** mean individual Director or Directors of the Board of the Company.
- xviii. **“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 authorized officer of the company as per the provisions contained in the Act.
- xix. **“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 (Act No 21 of 2000).
- xx. **“Enrolment number” means “Enrolment ID”** as defined in Section 2(1)(j) of the Aadhaar (Enrolment and Update) Regulation, 2016 which means a 28-digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.
- xxi. **“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.

- xxii. **"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.
- xxiii. **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- xxiv. **"(KYC Identifier)"** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- xxv. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the HFC or meeting the officials/ authorized representatives of the Company.
- xxvi. **"Officially Valid Document" (OVD)** means the following:
- A) Passport,
 - B) Driving license
 - C) Proof of possession of Aadhaar Number
 - D) Voter's Identity Card issued by the Election Commission of India,
 - E) Job card issued by NREGA duly signed by an officer of the State Government,
 - F) Letter issued by the National Population Register containing details of the name and address.

Explanations:

- i) Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India.
- ii) 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:-
 - a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - b) property or Municipal tax receipt, pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - c) 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.

The customer shall submit OVD with current address within a period of 3 months from the date of submitting the documents as specified above.

- iii) 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.)

- xxvii. **“On-going Due Diligence”** means regular monitoring of transactions in accounts to ensure that those are consistent with Company’s knowledge about the customers, customers’ business and risk profile, the source of funds / wealth.
- xxviii. **“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 RBI.
- xxix. **“Person”** has the same meaning assigned in the Act and includes:
- a. an individual,
 - b. a Hindu undivided family,
 - c. a Company,
 - d. a firm,
 - e. an association of persons or a body of individuals, whether incorporated or not,
 - f. every artificial juridical person, not falling within any one of the above persons
 - g. any agency, office or branch owned or controlled by any of the above persons.
- xxx. **“Politically Exposed Persons” (PEPs)** are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state owned corporations and important political party officials.
- xxxi. **“Principal Officer”** means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.
- xxxii. **“Video Based Customer Identification Process (V-CIP)”**; an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company 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 for the purpose of this Master Direction.
- xxxiii. **“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.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

xxxiv. **Certified Copy means** Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification can not 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 Company as per the provisions contained in the Act and the rules thereunder. 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

5. Know Your Customer (KYC) Policy

These Guidelines are framed keeping in mind the below mentioned four key elements:

- i. Customer Acceptance Policy
- ii. Risk management.
- iii. Customer Identification Procedures
- iv. Monitoring of Transactions

6. Money Laundering and Terrorist Financing Risk Assessment

Company will carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' annually 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 will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, company will take cognizance of the overall sector specific vulnerabilities, if any, that the regulator/supervisor may share with company from time to time.

- i. The risk assessment will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. Further, the periodicity of risk

assessment exercise will also be reviewed by the Risk Management Committee to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise.

- ii. The outcome of the exercise shall be put up to the Risk Management Committee to which power in this regard has been delegated and shall be available to competent authorities and self-regulating bodies.
- iii. The Company will apply a Risk Based Approach (RBA) for mitigation and management of the identified risk, and will have Board approved policies, controls and procedures in this regard. Further, Company will monitor the implementation of the controls and enhance them if necessary.

7. Designated Director & Principal Officer

- i. "Managing Director" and CEO of the Company shall be regarded as the "Designated Director" for ensuring overall compliance with the obligations imposed under the PML Act and the applicable Rules.
- ii. "Principal Officer", who is part of Compliance Function and reports to the Chief Compliance Officer, shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

Explanation: For this purpose, details of Designated Director & Principal Officer such as name, designation, address & contact details, will be communicated to RBI, NHB & FIU-IND.

8. Compliance of KYC Policy

It shall be the duty of all officers & employees of every department to observe the procedure and abide with the AML/KYC policy. The Senior Management team for KYC compliance will include all members who are one level below the Managing Director, as well as the functional heads and Principal Officer-AML. Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

- i. **The Designated Director** shall ensure overall compliance with the obligations with various KYC/AML/CFT norms in the Company.
- ii. **Chief Compliance Officer-** will be responsible for developing comprehensive KYC compliance programs tailored to the Company's unique structure and ensuring implementation thereof with the help of Senior Management.
- iii. **Chief Risk Officer-** will be responsible for Enterprise-wide risk assessment including ML/TF.
- iv. **Head, Operations-** will be responsible for obtaining and maintaining all KYC/CKYC/Re-KYC/V-KYC records from the customers as per prescribed guidelines by Regulatory Authorities, monitoring compliance at operations units, assigning correct risk category to the customer as per company's extant policy for risk categorization & assessment and closure of suspicious alerts as per extant procedure.

- v. **Head Internal Audit-** will be responsible for independent evaluation of the compliance of Company's policies and procedures, including legal and regulatory requirements. Concurrent/internal audit system will also be responsible to verify the compliance with KYC/AML/CFT policies and procedures and for submission of quarterly audit notes and compliance to the Audit Committee.
- vi. **Principal Officer –** will be responsible to ensure that the organization adheres to regulatory guidelines related to KYC and Anti-Money Laundering (AML) standards and sharing & reporting information to FIU as required under the law/regulations.
- vii. **Chief Technology Officer /Head IT -** will be responsible for effective system architecture & providing uninterrupted operations in accordance with the AML/KYC/CFT programme.
- viii. **Branch/Hub Managers:** will be responsible for implementing the KYC/AML guidelines in letter and spirit. They should promptly escalate any suspicious transaction to AML Team through e-mail/Transaction Monitoring tool.

9.Customer Acceptance Policy (CAP)

- i. The Company will accept a customer only after conducting the Customer Identification procedure. No transaction or account-based relationship will be undertaken without following the CDD procedure.
- ii. No account shall be opened in anonymous or fictitious/ benami name(s). The Company will ensure that the relevant documents are verified to ensure that no account is opened in anonymous or fictitious / benami name(s).
- iii. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the consumer or non-reliability of the documents/ information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- iv. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- v. Additional information, where such information requirement has not been specified in this KYC Policy of the Company then it will be obtained with the explicit consent of the customer.
- vi. CDD Procedure is followed for all the joint account holders, while opening a joint account.
- vii. Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to avail any other product or service from the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
- viii. The Company will put in place the suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the caution list issued by National Housing Bank and RBI, UNSC's sanctions lists as indicated in section (20) of the policy and any other list required from time to time

- ix. Circumstances, in which a customer is permitted to act on behalf of another person/entity, will be clearly spelt out in conformity with the established law and practices.
- x. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- xi. Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). The NBFC shall not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned shall duly record the reason(s) for rejection.
- xii. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- xiii. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- xiv. Where company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.
- xv. The Company will not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures i.e. it is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account will be taken by Senior Management after giving due notice to the customer explaining the reasons for such a decision.
- xvi. The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India.

10.Risk Management

The Company has ensured that an effective KYC program is in place and has established appropriate procedures and is overseeing its effective implementation. The program covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has been explicitly allocated within the Company to ensure that Company's policies and procedures are implemented effectively. For Risk Management, Company will have a risk-based approach which includes the following.

- i. Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.
- ii. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services 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.

- iii. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

11.Risk Categorization

Customers will be categorized under **Low**, **Medium** and **High-Risk** category, based on the assessment and risk perception of the Company. For high-risk customers, the Company will draw up additional precautions to be taken while dealing with such customers.

12.Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information while establishing a relationship. Company will obtain information stated below necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer.

The primary objectives of Customer Identification Procedure are:

- i. To verify the legal status of the customer/ entity through proper and relevant documents.
- ii. To verify that any person purporting to act on behalf of the customer, legal person/entity is so authorized and to verify the identity of such an authorized person.
- iii. To understand the ownership and control structure of the customer and determine who is the natural persons who ultimately has control over the management.

The Customer Identification Procedure shall be carried out by verifying Identity and residence proof of customers. The Company will follow the list of documents as enclosed in annexure C of the policy, which will be collected from the customers and will be verified at the time of establishing a relationship with the customer or while carrying out a financial transaction. The Company shall undertake identification of customers in the following cases:

- i. Commencement of an account-based relationship with the customer.
- ii. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- iii. Selling third party products as agents, selling their own products and any other product for more than INR 50,000/- (Rupees Fifty Thousand).
- iv. 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.

- v. In case of a customer who intends to place a deposit, the relationship is established at the time of receipt of a completed application form along with listed documents from the prospective depositor.
- vi. In case of a customer who intends to avail a loan, at the time the duly completed application form along with list of documents and other requirements from the prospective borrower.
- vii. In case of a customer who is a business associate (loan agent/ deposit agent), at the time when a duly completed application form is received for enrolment.
- viii. The company shall also obtain the source of funds/wealth documents from customers wherever deemed necessary.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company will rely on CDD done by a third party, subject to the following conditions:

- i. 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.
- ii. Adequate steps are taken by the Company to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- iii. 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 Prevention of Money-Laundering Act.
- iv. The third party shall not be based in a country or jurisdiction assessed as high risk.
- v. The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due-diligence measures as applicable, shall rest with the Company.

13. Customer Due Diligence (CDD) Procedure

Following will be the procedures for obtaining identification of customers:

While undertaking CDD, the Company will obtain the following information from an individual while establishing an account-based relationship with an 'individual' or dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity.

- i) the Aadhaar number where he is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act, or certified copy of an OVD containing details of identity and address, and one recent photograph; and
- ii) The Permanent Account Number (PAN)/equivalent e-document or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time., and
- iii) 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 company.
- iv) the Aadhaar number where,

- A) 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
- B) he decides to submit his Aadhaar number voluntarily to Company as 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; or
 - (ac) the KYC Identifier with an explicit consent to download records for CKYCR

Provided that where the customer has submitted,

- i) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.
- ii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under (Annexure B).
- iii) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under (Annexure B).
- iv) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with extant guidelines.

Explanation 1: Obtaining a certified copy by the Company shall mean comparing the copy of OVD so produced by the client with the original and recording the same on the copy by the authorized officer of the Company.

Explanation 2: The submission of Aadhaar by an individual as a KYC document in cases other than mentioned at (i) above may be provided out of own volition. customers, at their option, shall submit one of the OVDs

Explanation 3: The KYC documents for Individuals and Non-Individuals shall be obtained from Customers in terms of the requirements specified in annexure C of this policy.

Explanation 4: Company will, 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.

Explanation 5: Biometric based e-KYC authentication will be done by bank official/business correspondents/business facilitators.

Explanation 6: 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 and amendments made thereunder from time to time.

- v) In case the OVD furnished by the customer does not contain updated address, the deemed to be OVDs as defined in Section 4 (Definitions), can be taken into consideration for the limited purpose of proof of address (Provided further that the customer shall submit updated OVD with current address within a period of three months of submitting the above documents.)
- vi) Company may open accounts using Aadhaar OTP based e-KYC, in non-face-to-face mode in accordance with the applicable guidelines along with below mentioned additional measures.

In case of change of mobile number in such accounts, following process of due diligence will be diligently followed.

- Customer will place a formal physical request in person along with self -attested OVD for updation of mobile number in account in the branch. The request will also have an explicit reason for updation of new mobile number.
 - Respective officer of the company will verify the OVD, signature of the customer, photograph with the existing records and if required, the other KYC details also.
 - Respective officer will then process the request for change of mobile number after having obtained the prior approval from Head Operations.
 - An intimation regarding change in mobile number shall also be sent to the customer's registered email and by way of SMS (on his both old & new mobile numbers).
- vii) Video Customer Identification Process (V-CIP) The Company may undertake live V-CIP, to be carried out by any senior official of the company in accordance with the applicable guidelines.
- viii) A customer already having an account- based relationship with the Company, shall submit his Permanent Account Number or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the customer.
- ix) Provided further that if a customer having an existing account-based relationship with Company gives in writing to the company that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.
- x) Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard.
- xi) In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits will be allowed.

- xii) Where company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.
- xiii) The Company will duly inform the customer about this provision while opening the account.

14.Accounts of Politically Exposed Persons (PEPs):

Company will ensure that:

- i. sufficient information including information about the sources of funds/wealth, accounts of family members and close relatives is gathered on the PEP. Reasonable measures will be taken by the company for establishing the source of funds / wealth.
- ii. the identity of the person shall have been verified before accepting the PEP as a customer (whether as customer or beneficial owner)
- iii. the approval to open an account for a PEP is taken from senior management in accordance with the Customer Acceptance Policy.
- iv. all such accounts are subject to enhanced monitoring on an on-going basis.
- v. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, Senior Management's approval is obtained to continue the business relationship.
- vi. The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
- vii. These instructions shall also be applicable to family members or close associates of PEPs.

15.Ongoing Due Diligence

- i. Ongoing monitoring is an essential element of effective KYC-AML Programme. In this connection, Company will build up a risk- based transaction monitoring framework which will ensure the analysis and review of the 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, or transactions identified with current prevailing threats or typologies related to ML/TF or otherwise.
- ii. The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers. High risk accounts such as multi-level marketing (MLM), non-face-to-face etc, NRI etc will be kept under intensified monitoring.
- iii. Company will also identify the specific list of professions/categories which will have an over ridding effect to classify the customers as high- risk category irrespective of the score obtained under the other parameters. Eg: customers dealing in Crypto Currencies, Precious Metals, or have associations with high -risk countries etc.

- iv. Company will 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, the source of funds / wealth.
- v. For ongoing due diligence, Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring as when required.
- vi. A system of periodic review of risk categorization of accounts, once in six months, and the need for applying enhanced due diligence measures shall be put in place.
- vii. The risk categorizations of a customer and the specific reasons for such categorizations will be kept confidential and will not be revealed to the customer to avoid tipping off the customer.

16.Periodic Updation

Company will adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. Periodic KYC updation shall be carried out at least once in every **two years** for high-risk customers, once in every **eight years** for medium risk customers and once in every **ten years** for low-risk customers as per the following procedure:

i) For Individual Customers:

- a) **No change in KYC information:** In case of no change in the KYC information, a self declaration from the customer in this regard will be obtained through customer's email-id registered with the Company, mobile number registered with the Company, branch, digital channels or letter, etc.
- b) **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 the Company, mobile number registered with the Company, branch, digital channels or letter etc., and the declared address will be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.
- c) Further, Company, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation/ periodic updation as defined in Section 13 (vii).
- d) At the time of minor becoming major, Company will carry out fresh KYC as per current due diligence procedures.
- e) Aadhaar OTP based e-KYC in non-face-to-face mode may be used for updation/ periodic updation as per extant guidelines issued thereof.

ii) Customers other than individuals:

- a) **No change in KYC information:** In case of no change in the KYC information of the Legal entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer, through its email id registered with the company, digital channels, letter from an official authorized by the LE in this regard, board resolution and letter determining beneficial ownership etc.

- b) **Change in KYC information:** In case of change in KYC information, company will undertake the KYC process equivalent to that applicable for on- boarding a new LE customer.

iii) Additional measures: In addition to the above, Company will ensure that,

- a) that the KYC documents of the customer are as per the current CDD standards and extant guidelines outlined in detail in RBI KYC Master Directions, 2016 (Annexure C)
- b) customer's PAN details, if available, is verified from the database of the issuing authority at the time of updation/ 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 updation/periodic updation as also the date of updation of KYC details.
- d) In order to ensure customer convenience, company will make available the facility of updation/ periodic updation of KYC at any branch.
- e) Company will advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship/ account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This will be done within 30 days of the update to the documents for the purpose of updating the records at Company's end.
- f) The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options / channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation / reminder may, inter alia, contain easy-to-understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation / reminder shall be duly recorded in the Company's system against each customer for audit trail.

17. Monitoring of Transactions and maintenance and preservation of records:

Company will ensure maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. In this connection, company will maintain records of transactions and customer's data at each branch/hub and a consolidated record for all the branches taken together at the registered office of the Company as prescribed under provisions of Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005).

The Company will:

- i. maintain proper records of transactions, identification data of customers, Customer's address, details of transactions (date, nature & amount etc), parties involved in the transactions, and other related records of customers as defined in Rule 3 of PMLA.
- ii. maintain all necessary records of transactions between the company and the customer, for at least five years from the date of transaction.
- iii. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during business relationship, for at least five years after the business relationship is ended.
- iv. maintain all necessary records of all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
- v. maintain all necessary records of suspicious transactions whether or not made in cash.
- vi. maintain a record of a transaction of the deposit and loan accounts where there has been a receipt or payment in cash exceeding Rs.10 Lac per transaction; and also monitor and maintain record of deposits and loan accounts where there has been a series of cash transactions from the same customer during a month exceeding INR 10 Lac.
- vii. will ensure that in the event of ongoing investigation/ litigation, even if the accounts are closed, all records are preserved at least for five years after the closure of case.
- viii. will preserve records of STR data and other related correspondence with FIU/LEAs, at least for a period of 10 years from the date of reporting to authorities.
- ix. will ensure the swift availability of the identification records and transaction data to the competent authorities upon request.

18.Furnishing of information to the Director (FIU-IND):

Company will furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred in rule 3 & 8 of the PML (Maintenance of Records) Rules, 2005 in terms of rule 7 thereof. A copy of information furnished shall be retained by the 'Principal Officer' for the purposes of official record.

(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 reporting entities 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.)

- i. 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 will 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, will be made use of by the Company.

- ii. 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 misrepresented transaction beyond the time limit as specified in the said Rules shall be constituted as a separate violation.
- iii. Company will not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
- iv. Company will ensure that software throwing alerts, when the transactions are inconsistent with risk categorization and updated profile of the customers will be put in to use as a part of effective identification and reporting of suspicious transactions.
- v. Company's employees shall promptly furnish the required information to the Principal Officer AML /other appropriate staff as and when called for by him/her for further reporting to FIUIND. The background, including all documents /office records pertaining to such transactions, as far as possible, shall be examined by the Principal Officer -AML for recording assessment/ findings.

19. Reporting Requirement Under Foreign Account Tax Compliance Act (FATCA) And Common Reporting Standards (CRS)

Under FATCA and CRS, the Company, as Reporting Financial Institution, will adhere to the provisions of Income Tax Rules 114F, 114G and 114H and shall take following steps for complying with the reporting requirements:

- i. Register on the related e-filing 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.
- ii. Company will 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 – Company will 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 of Income Tax Rules.

- iii. Company will develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
- iv. Company will develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- v. In order to ensure the effective oversight, governance and adherence to FATCA (Foreign Account Tax Compliance Act) and CRS (Common Reporting Standard) compliance requirements under Rules 114F, 114G and 114H of Income Tax Rules, the Company will have the "High Level Monitoring Committee". The committee will play a pivotal role in ensuring timely compliance, international tax reporting obligations, enhancing internal controls, and mitigating regulatory risks.

The committee shall comprise the following officials of the company.

Designated Director - Chairman
Chief Compliance Officer - Member
Chief Information Officer - Member
Chief Finance Officer - Member
Head Operations - Member
Principal Officer - (Convener)

Roles and Responsibilities of the Committee

- Ensure timely compliance with FATCA & CRS obligations, including reporting to relevant authorities.
- Oversee the accuracy and completeness of customer and transaction data required for FATCA & CRS reporting.
- Ensure that IT systems and tools are capable of capturing, processing, and reporting the required FATCA & CRS information.
- Supervise the end-to-end processes related to FATCA & CRS, such as customer onboarding, self-certification, due diligence, and reporting.
- Identify risks associated with FATCA & CRS non-compliance and ensure that corrective measures are in place.
- Ensure that employees are trained on FATCA & CRS requirements and their roles in ensuring compliance.

Meeting Frequency

The High-Level Monitoring Committee shall meet on half yearly basis to review FATCA & CRS compliance status, resolve pending issues, and recommend any corrective actions.

- vi. Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

20.Requirements/obligations under International Agreements

i) **Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:**

- a) Company will ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, Company will 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:
- The **"ISIL (Da'esh) & Al-Qaida Sanctions List"**, established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at <https://scsanctions.un.org/ohz5jen-alqaida.html>
 - The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at <https://scsanctions.un.org/3ppp1en-taliban.htm>
 - Detailed obligatory directions related to blocked persons, Specially Designated Nationals or sanctioned individual/entity, as outlined in Master Directions, are added. {e.g. Unlawful Activities (Prevention) (UAPA) Act, 1967., Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005, UNSCs etc.)}

- b) Company will also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, will be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes will be taken into account by the Company for meticulous compliance.
 - c) Company will verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-SanctionsDPRK.htm> to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.
 - d) Company will undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.
 - e) 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 (MHA) as required under UAPA notification dated February 2, 2021
 - f) Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 will be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.
- ii) **Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**
- (a) Company will ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India.
 - (b) As per applicable guidelines, Company will ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
 - (c) Further, Company will run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
 - (d) In case of match in the above cases, Company will immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI.

- (e) Company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- (f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
- (g) In case an order to freeze assets under Section 12A is received by the Company from the CNO, Company, will, without delay, take necessary action to comply with the Order.
- (h) The process of unfreezing of funds, etc., shall be observed as per applicable guidelines in the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.
- (i) In addition to the above, Company will take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

iii) Jurisdictions that do not or insufficiently apply the FATF Recommendations

FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered.

- a) Company will apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
 - (b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.
 - (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.
 - e) Company will explore leveraging latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.
- iv) Company's policy framework ensures compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, Company may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

21. Other Measures

- i. A Unique Customer Identification Code (UCIC) shall be allotted while entering new relationships with individual customers as also the existing individual customers.
- ii. Company will ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of **NITI Aayog**. Company will register the details on the **DARPAN Portal** and will also maintain such registration records for a period of five years after the business relationship between the customer and the company has ended or the account has been closed, whichever is later.
- iii. Company will maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.
- iv. While considering the requests for data/ information from Government and other agencies, the Company will 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 transactions.
- v. Onboarding of High- Risk customer and reduction in the customer's risk classification from high to medium/low or from medium to low will be subject to the prior approval obtained from Senior Management.

22. Sharing KYC information with Central KYC Records Registry (CKYCR):

- i. The Company will capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised templates prepared for 'individuals' and 'Legal Entities' as the case may be. Company will adhere the guidelines as outlined by Central KYC 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.
- ii. The Company will upload the Know Your Customer (KYC) data with CERSAI in respect of new individual accounts opened on or after April 01, 2017, and records pertaining to accounts of LEs opened on or after April 1, 2021.
- iii. The details on Customer due diligence (CDD) procedure and sharing KYC information with C-KYCR will be as per the regulatory guidelines.
- iv. Once KYC Identifier is generated by CKYCR, company will ensure that the same is communicated to the individual/LE as the case may be. To download records from CKYCR, the Company will ensure to obtain an explicit consent from customer for KYC identifier.
- v. In terms of provision of Rule 9(1A) of the PML Rules, the Company will capture customer's KYC records and upload onto CKYCR **within 10 days** of commencement of an account-based relationship with the customer. Company will strictly adhere to the Operational Guidelines for uploading the KYC data have been released by CERSAI.
- vi. To ensure that all KYC records are incrementally uploaded on to CKYCR, company will upload/update the KYC data pertaining to accounts of individual customers and LEs opened

prior to the above-mentioned dates respectively, at the time of periodic updation or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the company obtains additional or updated information from any customer as per applicable guidelines or Rule 9 (1C) of the PML Rules, the company shall within **7 days** or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs us regarding an update in the KYC record of an existing customer, the company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by us.

- vii. For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Company will seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–
- a) there is a change in the information of the customer as existing in the records of CKYCR; or
 - b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - c) the validity period of downloaded documents has lapsed; or
 - d) the company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

23.Introduction of New Technologies

Company will identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Further, Company will ensure:

- i. to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- ii. adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

24.Hiring of Employees and Employee training:

- i. Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
- ii. Company has on-going employee KYC/AML/CFT training program for all members of staff. 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 KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.

- iii. Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Company shall also develop an environment which fosters open communication and high integrity amongst the staff.

25. Selling Third party products

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

- i. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required.
- ii. transaction details of sale of third-party products and related records shall be maintained as per extant guidelines.
- iii. 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.
- iv. transactions involving rupees fifty thousand and above shall be undertaken only by
 - a) debit to customers' account or against cheques; and
 - b) obtaining and verifying the PAN given by the account based as well as walk-in customers.
- v. Instruction at 'iv' above shall also apply to sale of Company's own products.

26. Adherence to Know Your Customer (KYC) guidelines by Company and persons authorised by Company including brokers/agents etc.:

- i. Persons authorized by the Company for collecting deposits and/or selling loan related products, their brokers/ agents or the like, will be fully compliant with the KYC guidelines applicable to the Company.
- ii. All information will be made available to the National Housing Bank to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by the Company including brokers/ agents etc. who are operating on their behalf.
- iii. The Company will ensure that the provisions of the PML Act, Rules framed thereunder and the Foreign Contribution (Regulation) Act, 2010, applicable, are adhered to strictly.
- iv. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

27.Enhanced Due Diligence (EDD) Procedure

- i) Any additional due diligence measures undertaken over and above the standard level of due diligence will be termed as Enhanced Due Diligence. For high- risk customers such as Nonface-to-face customers, PEP and relative and close associates of PEP and NRI etc, the Company will examine, as far as reasonably possible, the background and purpose of all complex, unusual patterns of transactions, which have no apparent economic or lawful purpose.
- ii) Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. EDD measures will be undertaken by the Company for non-face-to-face customer onboarding as detailed out in annexure D of the policy.
- iii) EDD will be applied to the customer level where the suspicion of money laundering or terrorist financing is prone to be high.
- iv) Risk classification of customer will be increased to High, if STR is filed on customer due to any reason.

Company Video Based Customer Identification Process (V-CIP)

The Company while undertaking V-CIP, will adhere to the following standards:

- 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, company will also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm as per **annexure C (CDD Measures for Sole Proprietary firms)**, 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.
- iii) Updation/ Periodic updation of KYC for eligible customers.

The company while undertaking V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

Company 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 will be housed in our own premises and the V-CIP connection and interaction will necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it will be ensured that the ownership of data in such model rests with the company only and all the data including video recording is transferred to the company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

- i) The Company will 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.
- ii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iii) 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.
- iv) The application will 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 us only. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- v) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly

upgraded. Any detected case of forged identity through V-CIP will be reported as a cyber event under extant regulatory guidelines.

vi) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

vii) The V-CIP application software and relevant APIs / webservises 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) Company will 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 the company specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs. Blinking of the eyes, smiling, frowning etc. shall not be a mandatory requirement for liveness check. Due cognizance of special needs of the customer shall be taken, if any, during liveness check.
- ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the company. However, in case of call drop / disconnection, fresh session shall be 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 will 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 workflow.
- 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 22, using the KYC identifier provided by the customer
 - d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker

- vii) Company will ensure to redact or blackout the Aadhaar number as explained in detail in Section 23. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP. Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, company will ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, company will ensure that no incremental risk is added due to this.
- viii) 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.
- ix) Company will 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 will be verified from the database of the issuing authority including through DigiLocker.
- x) The authorised official of the company will 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 will 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 this section but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.
- xiii) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(c) V-CIP Records and Data Management

- i) The entire data and recordings of V-CIP will be stored in a system / system located in India. Company will 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) The activity log along with the credentials of the official performing the V-CIP will be preserved.

Digital KYC Process

- i) The Company will develop an application for digital KYC process which will 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 the Company.
- ii) The access of the Application shall be controlled by the company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by company to its authorized officials.
- iii) The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
- iv) The company 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 company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- v) The Application of the company 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 color and no other person shall come into the frame while capturing the live photograph of the customer.
- vi) 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.
- vii) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- viii) 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.
- ix) 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 officers registered with the company shall not be used for customer signature. The Company will check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

- x)The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the company. 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.
- xi)Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the company, 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.
- x) The authorized officer of the Company will 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.;
- xi) On Successful verification, the CAF shall be digitally signed by authorized officer of the Company 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.

Sole Proprietary firms- For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.	
S. No.	Name of the Documents
1	Identification information of the individual (proprietor)
2	In addition to the above, any two of the following documents or the equivalent edocuments there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:
a.	certificate including Udyam Registration Certificate (URC) issued by the Government
b.	Certificate/licence issued by the municipal authorities under Shop and Establishment Act
c.	Sales and income tax returns
d.	CST/VAT/ GST certificate
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 Licence/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.
Company- For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained	
S. No.	Name of the Documents
1	Certificate of incorporation
2	Memorandum and Articles of Association
3	Permanent Account Number of the company
4	A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
5	Documents, as specified in section 13, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
6	the names of the relevant persons holding senior management position; and
7	the registered office and the principal place of its business, if it is different.
Partnership- 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	
S No.	Name of the Documents
1	Registration certificate

2	Partnership deed
3	Permanent Account Number of the partnership firm
4	Documents, as specified in section 13, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
5	the names of all the partners and
6	address of the registered office, and the principal place of its business, if it is different.
Trust-	
For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:	
S No.	Name of the Documents
1	Registration certificate
2	Trust deed
3	Permanent Account Number or Form No.60 of the trust
4	Documents, as specified in section 13, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
5	the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
6	the address of the registered office of the trust; and
7	list of trustees and documents, as specified in section 13, for those discharging the role as trustee and authorised to transact on behalf of the trust.
Unincorporated association or a body of individuals-	
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:	
S. No.	Name of the Documents
1	Resolution of the managing body of such association or body of individuals
2	Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
3	Power of attorney granted to transact on its behalf
4	Documents, as specified in section 13, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
5	Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding {other than customer onboarding in terms of Section 13 of the policy}

- a) In case Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of the KYC Master Direction, RBI 2016.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. **Transactions will be permitted only from the mobile number used for account opening.** Company will have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
- c) Apart from obtaining the current address proof, Company will verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) Company will obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

Note: When Company has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, when Company downloading and relying on such records from the CKCYR shall not be required to re-verify the authenticity of the customer's identity and / or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005.

The Company downloading and relying on KYC records downloaded from the CKCYR shall remain responsible for all aspects of CDD procedure and provisions of these Directions, except verification of identity and / or address of the customer.

Abbreviations

AI and ML- Artificial intelligence and machine learning
AML- Anti Money Laundering
BO- Beneficial Owner
CAP- Customer Acceptance Policy
CDD- Customer Due Diligence
CERT- in- Computer Emergency Response Team (CERT-In).
CFT- Combating the Financing Terrorism
CIDR- Central Identities Data Repository
CIP- Customer Identification Procedure
CKYCR- Central KYC Records Registry
CNO- Central Nodal Officer
CRS- Common Reporting Standards
CTR- Cash Transaction Reports
FATCA- Foreign Account Tax Compliance Act
FATF – Financial Action Task Force
FEDAI- Foreign Exchange Dealers' Association of India
FIU- IND- Financial Intelligence Unit - India
GST- Goods and Services Tax
KYC- Know Your Customer
LE- Legal entity
MHA- Ministry of Home Affairs
ML- Money Laundering
MLM- multi-level marketing
NGO- Non-governmental organization
NRI- Non-Resident Indians
OTP- One Time Password
OVD- Officially Valid Document
PAN- Permanent Account Number
PEP- Politically Exposed Persons
PIO- Persons of Indian Origin
PMLA- Prevention of Money-Laundering Act
PMLR- Prevention of Money-Laundering (Maintenance of Records) Rules
PPO- Pension Payment Orders
QR CODE- Quick Response Code
STR- Suspicious Transaction Reports
TF- Terrorist Financing
UAPA- Unlawful Activities (Prevention) Act
UCIC- Unique Customer Identification Code
V-CIP- Video Based Customer Identification Process
WMD- Weapons of Mass Destruction