KYC POLICY OF FINERGY TRANSPORT FINANCE LIMITED- APPROVED BY BOARD OF DIRECTORS AS ON 07.11.2024

1. Preamble:

Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board. Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

2. Objectives, Scope and Application of the Policy :

The primary objective is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. This policy also ensures for making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, etc. which in turn helps the Company to manage its risks prudently. The policy broadly has the following objectives

- To lay down explicit criteria for acceptance of customers
- To establish procedures to verify the bona-fide identification of individuals for commencement of financial relationship.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

3. Definitions:

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

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

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

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

v. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vi. "Designated Director" means a person designated by the company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors.

vii. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along

with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the company as per the provisions contained in the Act.

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

ix. "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.

x. "Group" – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

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

xii. "Officially Valid Document" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

- where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- 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;
    c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
    d) 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 three months of submitting the documents specified at 'b' above

xiii. 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.

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

xv. "Principal Officer" means an officer at the management level nominated by the company, responsible for furnishing information as per rule 8 of the Rules.

xvi. "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:

- 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
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have economic rationale or bona-fide purpose; or
- 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.

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

- opening of an account;
- deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- The use of a safety deposit box or any other form of safe deposit;
- Entering into any fiduciary relationship;
- Any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- establishing or creating a legal person or legal arrangement.

xviii. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

- Identification of the customer,
- verification of their identity using reliable and independent sources of identification,
- obtaining information on the purpose and intended nature of the business relationship, where applicable

- Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
- Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

xix. "Customer identification" means undertaking the process of CDD.

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

xxi. "Shell Bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xxii. 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 RE 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.

KNOW YOUR CUSTOMER STANDARDS

KYC procedures enable NBFCs to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The Company has framed its KYC policies incorporating the following **four** key elements:

1. Customer Acceptance Policy;

2. Customer Identification Procedures;

3. Monitoring of Transactions; and

4. Risk management.

1. **Customer Acceptance policy:**

The Company's Customer Acceptance Policy, which lays down explicit criteria for acceptance of customers, ensures the following aspects of the customer relationship:

a. No account is opened in anonymous or fictitious/benami name.

b. The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the borrower is not known or the Company is unable to

apply appropriate CDD measures, due to non-co-operation of the customer or non-reliability of the data/information furnished no transaction or account based relationship will be undertaken with such person / entity. However, the Company will have suitable built-in safeguards to avoid harassment of the customer.

c. No transaction or account-based relationship will be undertaken without following the CDD procedure.

d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

e. Additional information is obtained with the explicit consent of the customer.

f. The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account or avail any other product or service from the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

g. CDD Procedure is followed for all the joint account holders, while opening a joint account.

h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the MD issued by RBI.

j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

k. Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

l. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

m. Field Officers of the Company will ensure to record the Customer's accurate information such as Name, Husband's Name along with Client's Mother's or Father's Name, House No., Village, Post Office, Block/Tehsil, District, Pin Codes etc. as appearing in the identity and Address Proof produced before him.

The Company will prepare a profile for each new customer which may contain information relating to the customer's **identity, social/financial status, nature of business activity, information about clients' business and their location,** etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing the customer profile, the Company will seek only such information from the customer which is relevant and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose. The company shall ensure that the adoption of Customer Acceptance Policy and its implementation will not result in denial of the Company's services to the general public, especially to those who are financially or socially disadvantaged.

Where the 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.

2. **RISK MANAGEMENT**

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

a. Customers shall be categorised as ***low, medium and high-risk category***, based on the assessment and risk perception of the RE.

b. Broad principles be laid down for risk-categorisation of customers.

c. 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, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, 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.

d. 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.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

3. **CUSTOMER IDENTIFICATION PROCEDURE (CIP)**

The company shall undertake identification of customers before Commencement of an account-based relationship with the customer. Customer identification means identifying the customer and verifying her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each borrower and the purpose of the intended nature of business relationship. The Company will follow clear NBFC guidelines on the Customer Identification Procedure to be carried out at different stages, including establishing a financial relationship; carrying out a financial transaction, or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Apart from the above the customer identification procedures shall be applied to any transaction which shall be covered as per the KYC guidelines issued by the Reserve Bank of India from time to time. The Company shall perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The enhanced due diligence process shall also be applied by the company in case of suspicion of any money laundering or terrorist financing activities. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed shall be dynamic in nature and the parameters shall be changed based on the element of risk involved and the changes in the regulations as may be introduced from time to time by the regulatory authorities. The Customer Identification

Procedures shall be done internally by the company, however in case the company opts for CDD to be done by third parties, then the same shall be done in compliance with the extant regulations in this regard.

4. CUSTOMER DUE DILIGENCE PROCEDURE (CDD)

The company shall obtain the following information from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner:

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

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

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

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company:

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. The offline verification can be done in any manner as specified by UIDAI including the sharing of offline generated XML file or scan of QR code or sharing of masked Aadhar or Virtual ID. Where the customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, it shall be ensured that such customer redacts or blacks out his Aadhaar number through appropriate means.

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 of the customer with latitude and longitude as per digital KYC procedure specified under Annex I to RBI Master Directions on KYC, 2016.

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 Annex I to RBI Master Directions on KYC, 2016, copy of which is annexed to this policy as Part-I of Annexure 3. The company may also conduct CDD through V-CIP procedure as prescribed by RBI, copy of which is annexed to this policy as Part-II of Annexure 3. Provided that the company may obtain a certified copy

Provided that the company may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted. Provided further that accounts opened, opened using OTP based e-KYC shall not be allowed for more than one year unless prescribed identification has been carried out.

iv) Biometric based e-KYC authentication may be done by the company only when acting as business correspondents/business facilitators for banks.

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

(vi) The Company shall allot a Unique Customer Identification Code (UCIC)/ customer identification code or by whatever name called, while entering into new relationships with individual customers as also the existing customers. (vii) 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 terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision.

(vii)Identification of Beneficial Owner: The Prevention of Money Laundering Rules, 2005 and as amended in 2013 requires every banking company, and financial institution, to identify the beneficial owner and take all reasonable steps to verify his identity. Beneficial Owner (BO) is defined as follows:

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means. Explanation- For the purpose of this sub-clause1. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company. 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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

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

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

V-CIP

The company may undertake V-CIP to carry out:

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

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:

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. the Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, the Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps are taken to verify the founder managers/ directors and the beneficiaries, if defined. The Company is vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. The Company examines the control structure of theentity, determine the source of funds and identify the natural persons who have a c o ntrolling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

(viii) Simplified procedure for opening certain accounts:

In case a person who desires to open an account is not able to produce documents, as specified in point (i) above, the company may, at its discretion open accounts subject to the following conditions:
a. The company shall obtain a self-attested photograph from the customer.

b. The designated officer of the company shall certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

c. The account shall remain operational initially for a period of twelve months, within which complete CDD procedure shall be carried out.

d. Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.

e. The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

f. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

g. The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. However, the extent of monitoring will depend on the risk sensitivity of the customer. Since the Company does not have any deposit accounts of its customers, this situation will hardly arise, but the Company will in any case pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. The Company will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due

diligence measures. The Company will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002 (and the Amended Act, 2009). It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under section 12 of the PML Act, 2002 (and the Amended Act, 2009), is reported to the appropriate law enforcement authority.

Introduction of New Technologies

The Company shall pay adequate attention to any money laundering and financing of terrorism threats that may arise from new or developing technologies and it shall ensure that appropriate KYC procedures issued from time to time are duly applied before the introduction of new products/services/ technologies. The Company neither has deposit accounts nor is it permitted by RBI to accept deposits from customers, therefore many of the risks presented by the introduction of new technology such as internet banking, mobile banking or transactions that do not require physical presence of the parties etc., are not faced by it. However, the Company pays special attention to any money laundering threats that may arise from new or developing technologies including internet and mobile banking, on-line transactions that might favour anonymity, and take measures, if needed, to prevent its use in money laundering schemes. As per guidelines issued by RBI following are the important Software Application controls and risk mitigation measures that the Company has implemented:

a) Each application should have an owner which will typically be the concerned business function that uses the application.

b) Some of the roles of application owners include:-

- Prioritizing any changes to be made to the application and authorizing the changes.
- Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements.
- Ensuring that adequate controls are built into the application through active involvement inthe application design, development, testing and change process - Ensuring that the application meets the business/functional needs of the users
- Ensuring that the information security function has reviewed the security of the application
- Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
- Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements
- Ensuring that the Change Management process is followed for any changes in application
- Ensuring that the new applications being purchased/developed are in accordance with the InformationSecurity policy
- Ensuring that logs or audit trails, as required, are enabled and monitored for the applications

c) All application systems should be tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the Company and regulatory and legal prescriptions/requirements. Robust controls should be built into the system and reliance on any manual controls has been minimized. Clear instructions should be issued to ensure the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.

d) The Company has to incorporate information security at all stages of software development to improve software quality and minimize exposure to vulnerabilities. Besides business functionalities,

security requirements relating to system access control, authentication, transaction, authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are clearly specified at the initial stages of system development/acquisition. A compliance check against the Company's security standards and regulatory/statutory requirements should be put in place.

e) All application systems need to have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard.

f) Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, must provide for detailed audit trails/ logging capability.

g) The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it is to be ensured that they are not tampered with.

h) Access should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties has to be enforced.

i) There should be controls on updating key 'static' business information like customer master files, parameter changes, etc.

j) Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment, authorization from an appropriate authority, implementation, testing and verification of the change done.

k) Potential security weaknesses / breaches (for example, as a result of analysing user behaviour or patterns of network traffic) should be identified.

l) There should be measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.

M) Applications must not allow unauthorized entries to be updated in the database. Similarly, applications must not allow any modifications to be made after an entry is authorized. Any subsequent changes must be made only by reversing the original authorized entry and passing a fresh entry.

n) Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.

o) Access to the database prompt must be restricted only to the database administrator.

p) Robust input validation controls, processing and output controls have to be built into the application.

q) There is a procedure in place to reduce the reliance on a few key individuals.

r) Error / exception reports and logs are reviewed and any issues is remedied /addressed at the earliest.

s) For all critical applications, either the source code is received from the vendor or a software escrow agreement is put in place with a third party to ensure source code availability in the event the vendor goes out of business. It is ensured that product updates and programme fixes are also included in the escrow agreement.

t) In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access

controls based on 'need to know' and robust change controls. The Company should be in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees orother persons.

u) An application security review/testing, initially and during major changes, needs to be conducted using a combination of source code review, stress loading, exception testing and compliance review to identify insecure coding techniques and systems vulnerabilities to a reasonable extent.

v) Critical application system logs/audit trails also need to be backed up as part of the application backup policy.

w) Robust System Security Testing, in respect of critical e-banking systems, needs to incorporate, inter-alia, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. These need to be carried out at least on annual basis.

PERIODIC UPDATION OF KYC FOR EXISTING ACCOUNTS

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. ***Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers***. Keeping in view the business of the company wherein the loan account is repaid in shorter span of time, and the borrowers falling in low risk, the requirement of updation may not arise. However, in case the company identifies any customer as high risk or medium risk customer, then it shall comply with the directions of the RBI regarding periodic updation, as follows:

a) **Individual Customers**:

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

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

Further, the company, at its option, 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 periodic updation.

B) **Customers other than individuals**

i) No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the company, mobile application of the company), letter from an official authorized by the LE in

this regard, board resolution etc. Further, the company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

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

iii) Additional measures: In addition to the above, the company shall ensure that,

- The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the company has expired at the time of periodic updation of KYC, the company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- Customer's PAN details, if available with the company, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- In order to ensure customer convenience, the company may consider making available the facility of periodic updation of KYC at any branch.
- The company shall ensure that its KYC processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements. The transactions in existing customers would be continuously monitored for any unusual pattern in the operation of the accounts. Further if an existing customer is KYC compliant and she desires to open another account, there shall be no need for any fresh customer due diligence exercise.

The transactions in existing customers would be continuously monitored for any unusual pattern in the operation of the accounts. Further if an existing customer is KYC compliant and she desires to open another account, there shall be no need for any fresh customer due diligence exercise.

Applicability to branches:

The above guidelines shall also apply to all the branches of the company located in India or the branches which may be located abroad. However, in case any local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank of India.

Secrecy Obligations and Sharing of Information:

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship with the customer.

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

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

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of the company requires disclosure and

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

Hiring of Employees and Employee Training:

a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

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

PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002 - OBLIGATIONS OF THE COMPANY INTERMS OF RULES NOTIFIED THEREUNDER

a) Appointment of principal officer

For the purpose of this policy and compliance of KYC/AML/CFT regulations, Mrs. K Jayalakshmi, Company Secretary shall act as Principal Officer and put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. For the purpose of this policy and the compliance of KYC/AML/CFT regulations, any other officer as appointed by Managing Director be designated as 'Principal Officer' shall act as the Principal Officer of the company. The name, designation and address of the Principal Officer has been duly communicated to the Director, Financial Intelligence Unit – India (FIUIND). As per the NBFC guidelines, the Principal Officer will be located at the corporate office and will be responsible for ensuring compliance, monitoring transaction, and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

b) Appointment of Designated Director

For the purpose of this policy and the compliance of KYC/AML/CFT regulations, Mr. Gowthaman, Managing Director shall be the Designated Director. The name, designation and address of the Designated Director has been duly communicated to the Director, Financial Intelligence Unit – India (FIU-IND). If the Director-FIU, in the course of any inquiry, finds that a reporting entity or its designated director (Mr Gowthaman) on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

(a) issue a warning in writing; or (b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; (or)

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; (or)

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

In view of the above, the Company should nominate a Director on their Boards as "designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

c) Maintenance of records of cash transactions and suspicious transactions:

The Company shall maintain proper record of transactions as mentioned below:

i. All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.

ii. All series of cash transactions integrally connected to each other which have to be valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;

iii. all cash transactions where forged or counterfeit currency notes or bank notes have to be usedas genuine and where any forgery of a valuable security has taken place.

iv. All suspicious transactions whether or not made in cash.

The Company shall maintain the following information in respect of the above cash transactions:

- the nature of the transactions;
- The amount of the transaction and the currency in which it was denominated;
- The date on which the transaction was conducted; and
- The parties to the transaction.

d) Record Retention:

The following steps shall be taken for maintaining, preserving and reporting of customer account information, with reference to provisions of PML Act and Rules. The company shall:

- Maintain all necessary records of transactions with the customer, for at least five years from the date of transaction;
- Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- Make available the identification records and transaction data to the competent authorities upon request;
- Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
- Maintain records of the identity and address of their customer, and records in respect of transactions in hard or soft format.

e) Filing of Suspicious Transaction Report (STR) to FIU-IND

Any suspicious transactions, counterfeit transactions and any cash transactions of Rs.10 lakhs or above, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month, shall be identified. Further, the Principal officer shall, within the prescribed timelines, furnish information of such transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the following address in the formats prescribed in this regard including the electronic filing of reports.

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021

Provided that where the Principal officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time. The Company shall not put any restriction on operations in the accounts where a suspicious transaction report (STR) has been filed. The Company shall keep the fact of furnishing of STR strictly confidential and shall ensure that there is no tipping off to the customer at any level.

f) Uploading of KYC Data on CERSAI Platform

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR. In terms of provision of Rule 9(1A) of PML Rules, the company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
(b) The company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prescribed by CERSAI for 'Individuals' and 'Legal Entities' (LEs), as the case may be.

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

(d) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the specified dates, at the time of periodic updation or earlier, when the updated KYC information is obtained/received from the customer.

(e) The company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(f) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the company, with an explicit consent to download records from CKYCR, then the company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

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

COMBATING FINANCING OF TERRORISM (CFT)

In terms of PMLA Rules, suspicious transaction should include transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Though keeping in view the size of loan and type of customers the company is dealing with the chances of accounts with terror links are very low, however the Company has developed a suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority. As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates the Company ensures to update the consolidated list of individuals and entities as circulated by Reserve Bank. The Company also ensures that before opening any new account the name/s of the proposed customer does not appear in the list. Further, the Company has put in place procedures to scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI , FIU-IND along with Ministry of Home Affairs.. The Company shall take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. The Company shall, in addition to FATF Statements circulated by Reserve Bank from time to time, also consider publicly available information for identifying such countries, which do not or insufficiently apply the FATF Recommendations. The Company should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries.

1. Monitoring

Ongoing monitoring is an essential element of effective KYC procedures. The Company should examine 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. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents be retained and made available to Reserve Bank/other relevant authorities, on request. The Company applies enhanced due diligence measures on high risk customers.

2. Operation of Bank Accounts and money mules

The guidelines covered under this policy for opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules."

3. Accounts of Politically Exposed Persons (PEPs)

Customer Due Diligence (CDD) measures to be made applicable to Politically Exposed Person (PEP) and their family members or close relatives. Before establishing any relationship with the PEPs sufficient information including information about the sources of funds, accounts of family members and close relatives shall be gathered and the identity of the person shall be verified before accepting the PEP as a customer. The decision for entering into any business relationship with a PEP, shall be taken at a senior level within the scope of Customer Acceptance policy of the company. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. The similar procedure shall be applicable in case of accounts of PEP who are resident outside India. The instructions are also applicable to accounts where PEP is the ultimate beneficial owner. Further, in regard to PEP accounts, the Company has appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

4. Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In such cases, the Company may also require the first payment to be effected through the customer's KYC Compliant account with another bank which, in turn, adheres to similar KYC standards. In the case of crossborder customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

5. Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. The Company shall gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, the Company should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards wishes to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO the Company while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

6. Shell Banks :

The Company shall not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group).

7. Obligations under International Agreements:

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they do not have any account 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:

(a) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htd ocs/resources/xsl/en/al-qaida-r.xsl

(b) The"1988 Sanctions List", consisting of individuals (Section A of the consolidated list)