KYC AND AML POLICY
OF

R-SECURED
FINANCE & CAPITAL PVT. LTD

RSECURED FINANCE & CAPITAL PRIVATE LIMITED

KYC AML POLICY

SUMMARY OF POLICY

Policy Name	**Know Your Customer and Anti Money Laundering Policy**
Issue and Effective date	29/04/2024
Owner / Contact	**Compliance Department**
Approver	**Board of Directors**
Annexures	• **Customer Identification Process- Annexure-A** • **Indicative list for risk categorization of customers as- Annexure-B** • **List of KYC documents for different type of customers as- Annexure-C** • **Process of reporting of suspicious transactions Annexure- D** • **Business Partner Due Diligence Procedure - Annexure-E**

SUMMARY OF THE POLICY

S. No.	Particulars
1.	Introduction
2.	Purpose
3.	Definitions
4.	Constitution of Senior Management
5.	Customer Education
6.	Outsourcing
7.	Scope
8.	Hiring and Training
9.	Key Elements
	a. Customer Acceptance Policy ("CAP")
	b. Customer Identification Procedures ("CIP")
	c. Monitoring of Transactions
	(i) Provisions under PMLA
	(ii) Maintenance of records of transaction
	(iii) Monitoring & reporting of transactions
	d. Risk management
10.	Appointment of Principal Officer (PO)
11.	Appointment of Designated Director
12.	Money Laundering and Terrorist Financing Risk Assessment
13.	Identification of Beneficial Ownership
14.	Record Retention
15.	Reporting to Central KYC Registry (CKYCR)
16.	Reporting Requirements to Financial Intelligence Unit – India.
17.	Reporting Requirement under Foreign Account Tax Compliance Act (FATCA).
	Annexure-A- Customer Identification Process
	Annexure-B- Indicative list for risk categorization of customers
	Annexure-C- List of KYC documents for different type of customers
	Annexure-D- Process of reporting of suspicious transactions
	Annexure-E - Business Partner Due Diligence Procedure

KYC AML POLICY

1. Introduction

Reserve Bank of India has issued Master Direction- Know Your Customer (KYC) Direction, 2016 including 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.

The policy has been framed in accordance with Reserve Bank of India (Know Your Customer (KYC) revised master direction vide circular no. DBR.AML.BC. No.81/14.01.001/2015-16 dated May 10, 2021 and terms of the provisions of Prevention of Money-Laundering Act, 2002 and PMLA rules thereunder.

This Policy envisages the establishment and adoption of measures and procedures relating to KYC, AML and CFT for the RSFCPL in accordance with the requirements prescribed by RBI and modified from time to time

Accordingly, in compliance with the guidelines issued by RBI from time to time, the Board of Directors (the Board) of **RSecured Finance and Capital Private Limited (RSFCPL)** has adopted the policy named as Know Your Customer ('KYC') / Anti-Money Laundering (''AML'') policy as per norms prescribed by Reserve Bank of India ("RBI").

This policy is applicable to all categories of products and services offered by the Company.

This Policy was further amended by the Board of Directors at their meeting held on 29th April 2024.

2. Purpose

The primary objective of "***Know Your Customer***" (KYC) and Anti-Money Laundering (''AML'') policy is to prevent RSecured Finance and Capital Private Limited (RSFCPL) from being used, intentionally or otherwise, by unscrupulous elements for fraudulent/money laundering and terrorist financing activities as enunciated in the "***Customer Acceptance Policy*** "of RSFCPL.

KYC procedures also enable the Company to know/understand its customers and their financial dealings better which in turn help them manage the risks prudently.

RSFCPL will follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions as per provisions of Prevention of Money-Laundering Act, 2002 and rules framed thereunder.

These guidelines are issued to reinforce the existing checks and controls developed by the RSFCPL and to ensure due diligence while starting/extending relationships with/to a new/existing customer.

Furthermore, in compliance with RBI guidelines, the main objective of this policy is to enable the Company to have positive identification of its customers. The RBI guidelines mandate making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc., which in turn helps the Company manage its risks prudently.

3. Definitions

a. **"Aadhaar 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', means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information after verifying the information in such manner as may be specified in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

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.

b. **"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.

c. **"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;

d. **Beneficial Owner (BO):** 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 25 per cent of the shares or capital or profits of the Company.**
- **"Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by their shareholding or management rights or shareholder's agreements or voting agreements.**

- 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.

- 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.**

e. **"Board"** means **Board of Directors** of the Company.

f. **"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;

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

h. **"Certified Copy"** means comparative copy of the proof of possession of an Aadhaar number where offline verification cannot be carried out or officially valid document produced by the customer with the original and recording the same on the copy by the authorized officer of the company.

i. **"Company**" means "**RSecured Finance and Capital Private Limited (RSFCPL)"**

j. **"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;

k. "Designated Director" means Managing Director or whole-time Director or executive director or director, 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. –

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

ii. "Directors" mean individual Director or Directors on the Board of the Company.

m. **"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.

n. **"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.

o. **"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.

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

q. **"Officially valid document" (OVD)** means the following: Passport, driving license, Proof of possession of Aadhaar Number, Voter's Identity Card issued by the Election Commission of India, Job card issued by NREGA duly signed by an officer of the State Government, Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

"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;".

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.

T. "Person" has the same meaning assigned in the Act and includes: an individual, a Hindu undivided family, a Company, a firm, an association of persons or a body of individuals, whether incorporated or not, every artificial juridical person, not falling within any one of the above persons any agency, office or branch owned or controlled by any of the above persons

s. **"Principal Officer"** means a Senior officer nominated by RSFCPL, responsible for furnishing information as per rule 8 of the Rules;

t. **"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:

i. 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.

u. **"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.

v. **"Video based Customer Identification Process (V-CIP)"** means a method of customer identification by an official of the company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

w. **"Yes/No authentication facility",** as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing "Yes" or "No", along with other technical details related to the authentication transaction, but no identity information.

Terms bearing meaning assigned above, unless the context otherwise requires, shall bear the meanings assigned to them below:

(i) **"Common Reporting Standards" (CRS)** means reporting standards set for implementation of multilateral agreements signed to automatically exchange information based on Article 6 of the Convention on Mutual AAFPL instructive Assistance in Tax Matters.

(ii)**"Customer"** means a person who is engaged in a financial transaction or activity with a company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

(iii)**"Walk-in Customer"** means a person who does not have an account-based relationship with the company but undertakes transactions with the Company. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner "Customer identification" means undertaking the process of CDD.

(iv)**"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 KYC and AML Policy substantial ownership interest.

(v)**"IGA"** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

(vi)**"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

(**vii) "Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

(viii)**"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

(ix)**"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.

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

(xi)**"Regulated Entities" (REs)** means: all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs)/State and Central Cooperative Banks (St CBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks' All India Financial Institutions (AIFIs) All Non-Banking Finance Companies (NBFC)s, Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs). All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) all authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

(xii)**"Simplified procedure**" means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by the RE and who do not possess any of the six officially valid documents, with the alternate documents prescribed under the two provisos of Section 3(a)(vi) of this Directions.

(xiii) **"Shell bank"** means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

(xiv) **"Wire transfer"** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to make an amount of money available to a beneficiary person at a bank.

(xv) **"Domestic and cross-border wire transfer":** When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer. 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.

(xvi) "Offline verification" Means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations.

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.

4. Constitution of Senior Management

As required under clause of KYC master Direction issued by RBI, board has constituted Senior Management for effective implementation and Independent periodic evaluation of KYC AML Policy and Senior Management comprises Chief Compliance Officer and members of board of directors.

The responsibility of effective implementation and Independent periodic evaluation of KYC AML policies and its procedures is with the Senior Management which may delegate further to the compliance department team.

5. Customer Education

For implementing KYC policy, the Company shall have to seek personal and financial information from the new and intended customers at the time they apply for availing the loan facilities. It is likely that any such information, if asked from the intended customer, may be objected to or questioned by the customers. To meet such a situation, it is necessary that the customers are educated and appraised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company.

For this purpose, all the staff members with whom the customers will have their first interaction / dealing will be provided special training to answer any query or questions of the customers and satisfy them while seeking certain information in furtherance of KYC Policy. To educate the customers and win their confidence in this regard, the Company may arrange printed materials containing all relevant information regarding KYC Policy and anti-money laundering measures. Such printed materials will be circulated amongst the customers and in case of any question from any customer, the Company staff will attend the same promptly and provide and explain the reason for seeking any specific information and satisfy the customer in that regard.

6. Outsourcing:

RSFCPL shall not outsource Decision making function of determining compliance with KYC Norm while sanction for loans accordance to the notification no DNBR.PD.CC. No.090/03.10.001/2017-18 dated November 09, 2017 issued by the Reserve bank of India.

Further business partner due diligence procedure is annexed with this policy as **Annexure-E.**

7. Scope

This Policy shall be applicable for all new and existing customer and business partner relationships of RSFCPL.

8. Hiring and Training

HR, Legal, Compliance and Operations department to arrange an on-going training program for the different categories of members of staff and to ensure that they are adequately trained in KYC/AML procedures. Specific training program is required from a focus point of view for field staff, processing staff, compliance staff and audit staff. Effectiveness of the training to be

documented with the training department. It is crucial that all those concerned fully understand the rationale behind the KYC/AML policies and implement them consistently.

9. Key Elements

RSFCPL has framed its KYC policy incorporating the following four key elements: -

a) **Customer Acceptance Policy;**
b) **Customer Identification Procedures;**
c) **Monitoring of Transactions; and**
d) **Risk management.**

For the purpose of the KYC policy, a 'Customer' is defined as per Clause 3 i.e., Definitions.

a) Customer Acceptance Policy (CAP)

RSFCPL will follow norms and procedures in relation to its customers who approach the Company for availing financial facilities. While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms will be adhered by the Company:

(i) No loan account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account i.e., Benami Account. The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.

(ii) Circumstances, in which a customer is permitted to act on behalf of another person /entity, shall be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by intermediary in a fiduciary capacity.

(iii) The Company shall apply CUSTOMER DUE DILIGENCE (CDD) measures at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a Reporting Entity (RE) desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.

(iv) CDD Procedure is followed for all the joint account holders, while opening a joint account.

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

(vi) The customer profile contains mandatory information to be sought for KYC purpose relating to customer's identity, address, social/financial status, nature of business activity, information about the 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 to the risk category 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 maintain secrecy regarding customer information except where the disclosure is under compulsion of law, there is a duty to the public to disclose, the disclosure is made with express or implied consent of the customer.

(vii) The Company shall ensure that the identity of the customer does not match with any person or entity whose name appears in the sanction lists circulated/prescribed by RBI from time to time

(viii) The intent of the Policy is not to result in denial of financial services to the general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

(ix) The Company shall not open any account or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:

- The Company is unable to verify the identity of the customer.
- The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity.
- Information furnished by the customer does not originate from reliable sources or appears to be doubtful due to lack of supporting evidence.
- Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.

(x) Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

(xi) The Risk Team shall, at the time of approving a financial transaction/activity, or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer. For co-lending loans, this shall be verified by the NBFC partner. The Company shall however maintain a repository of KYC documents of borrowers under the co-lending program as well.

Risk Level Categorization

1) The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk. The risk categorization would depend on various factors such as the function of the industry the

borrower operates in, the geography in which the borrower operates, the shareholding pattern of the entity etc.

2) The profile of new customers will be prepared on a risk categorization basis. Such profile will contain the following information about the new customers:
   1. Customer's Identity.
   2. Social/Legal and financial status of the customer.
   3. Nature of the business activity.
   4. Information about the business of the customer's clients and their locations.

3) There will be level-wise categorization of customers i.e., Level-I, Level-II and Level-III. Such levels will be decided based on risk element involved in each case which will be determined by considering the following information submitted by the customer:
   1. Nature of business of the Customer and of his clients
   2. Work place of Customers and of his clients
   3. Country of Origin
   4. Source of funds
   5. Volume of business six-monthly/annual turn-over
   6. Social/Legal and financial status
   7. Quantum and tenure of facility applied for and proposed schedule for repayment of loan

4) Information to be collected from the customers will vary according to categorization of customers from the point of view of risk perceived. However, while preparing the customer profile the Company shall seek only such information from the customer which is relevant to the risk category and is not intrusive to the customer. Any other information from the customer should be sought separately with his/her consent and after opening the account.

5) For risk categorization, individuals (other than High Net Worth) and entities whose sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorized as low risk or Level-I category. Normally Level-I customers would be
   1. Well governed corporations.
   2. Salaried employees having definite and well-defined salary structure.
   3. Employees of Government Departments or Government owned companies.
   4. Statutory bodies.
   5. Self-employed individuals, however with regular income and good credit behavior.

6) Cases where the Company is likely to incur higher than average risk will be categorized as **medium or high-risk customers** and will be placed in **medium or highrisk category i.e. Level-II or Level-III** category. While placing the customers in the above categories, the Company will give due consideration to the following aspects:
   1. Customer's background,

2. Country of his origin,
3. Nature and location of his business activities,
4. Sources of funds and profile of customer's clients etc.

In such cases, the Company will apply higher due diligence measures keeping in view the risk level.

7) Special care and diligence will be taken and exercised in respect of those customers who happen to be high profile and/or Politically Exposed Persons ("PEP") within or outside the country. Such persons will include:

1. Foreign Delegates or those working in Foreign High commissions or Embassies,
2. Senior Politicians,
3. Senior Judicial Officers,
4. Senior Military Officers,
5. Senior Executives of State-Owned Corporations and
6. Officials of important and leading political parties

8) The extent of due diligence requirements will vary from case to case as the same will depend upon the risk perceived by the Company while granting credit facilities to the customers.

For the purpose of preparing the customer profile only such relevant information from the customers will be sought based on which the Company can easily decide about the risk category in which the customers are to be placed. Ordinarily, the customer profile maintained by the Company will be kept confidential except for cases where the customer himself allows and/or gives consent for the use of the information given in customer profile / application form for offering other products / services of other companies / entities belonging to the Company's group or any other legal entity with whom the Company is having any business tie-ups. However, while taking any such permission or consent of the customer for using his above referred information provided to the Company, it will be ensured that such permission / consent of the customer is unambiguous and explicit

RSFCPL has formulated a list and their respective risk categories of customers. The same is attached as Annexure-B to this Policy.

b). Customer Identification Procedure ('CIP')

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. RSFCPL will obtain information stated under annexure-c necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of the relationship.

Being satisfied means that RSFCPL must be able to satisfy the competent authorities like RBI 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. For customers that are legal persons or entities,

Customer identification requirements in respect of a few typical cases, especially, legal persons

requiring an extra element of caution.

According to the regulatory norms, RSFCPL should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows' who the beneficial owner(s) is/are.

RSFCPL should ensure that the identity of the customer, including the beneficial owner, is done based on disclosures by the customers themselves.

RSFCPL shall comply with section 11 of PML Act, 2002 to verify the identity of their customers and beneficial owners.

An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

- Verify the identity of any Person transacting with the Company to the extent reasonable and practicable
- Maintain records of the information used to verify a customer's identity, including name, address and other identifying information and
- Consult sanctions lists/ FATF statements of known or suspected terrorists:
- The Company shall ensure that, in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, the Company does 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) and whose names appears in the sanctions lists circulated by Reserve Bank of India/

The Company may ensure the aforesaid, verifying the name of person or entity through the website of the concerned entity or through the service provider, who provide the said service of third party verification, in compliance applicable provisions/guideline of Reserve Bank of India/National Housing Bank, the Prevention of Money Laundering Act and rules made thereunder in this regard. Details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list, shall be treated as suspicious and reported to the FIU-IND, apart from advising Ministry of Home Affairs as required under UAPA notification.

The Credit Head, will be responsible to ensure that the name of Borrower is not reflecting in the aforesaid list.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

A detailed customer identification Procedure is given under **Annexure-A.**

An indicative list of the nature and type of documents/information that may be relied upon for customer identification are provided as **Annexure-C.**

Customer Due Diligence Procedures ("CDD")

Procedure for obtaining Identification Information

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

Part I - CDD Procedure in case of Individuals. RSFCPL shall apply the following procedure on an individual while establishing an account- based relationship:

(i) Obtain information as mentioned under Section 15; and

(ii) Such other documents pertaining to the nature of business or financial status specified by the company in their KYC policy.

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

Part II - CDD Measures for Sole Proprietary Firms

For opening a loan account in the name of a sole proprietary firm, identification information as mentioned under Section 15 in respect of the individual (proprietor) shall be obtained. –

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

- Registration certificate
- Certificate/license issued by the municipal authorities under Shop and Establishment Act.
- Sales and income tax returns.
- CST/VAT/GST certificate (provisional/final)
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
- License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
- Utility bills such as electricity, water, and landline telephone bills

- In cases where RSFCPL is satisfied that it is not possible to furnish two such documents, RSFCPL

may, at their discretion, accept only one of those documents as proof of business/activity.

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

Part III**- CDD Measures for Legal Entities** –

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

- Certificate of incorporation.
- Memorandum and Articles of Association.
- Permanent Account Number of the company,
- resolution from the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf,
- one copy of an officially valid document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

Part IV. CDD Measures for partnership firm

For opening a loan account of a partnership firm, certified copy of each of the following documents or the equivalent e-documents thereof shall be obtained:

- Registration certificate
- Partnership deed.
- Permanent Account Number of the partnership firm; and
- One copy of an officially valid document containing details of identity and address, one recent photograph and Permanent Account Number or Form No.60 of the beneficial owner, managers, officer.

c). Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. RSFCPL 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 of activity.

However, the extent of monitoring will depend on the risk sensitivity of the account. Since RSFCPL may not have any deposit accounts, this situation will not arise, but RSFCPL shall pay special attention to depleting financial ratios, adequacy of collaterals etc.

RSFCPL will put in place a system of half-yearly review of risk categorization of all outstanding accounts and the need for applying enhanced due diligence measures.

RSFCPL will ensure that record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002 and Rule 3, 4, and 5 of the PMLA Rules 2005 (Refer Point 8 for maintenance of records and Point 9 for preservation of records under the PML act) in a separate register at the registered office of RSFCPL in physical or electronic form and make

it available to the regulatory and investigating authorities. 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 Rule 3, 4, and 5 of the PMLA Rules 2005 is reported to the appropriate law enforcement authority.

PROVISIONS UNDER PMLA

As per the provisions of Rule 9 of the Prevention of Money Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

·at the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship and

·in all other cases, verify identify while carrying out:

- 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,
- Any international money transfer operations.

In terms of provision to rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn. Abiding by the provisions of Rule 9, the Company shall identify the beneficial owner and take all the reasonable steps to verify his identity. The said Rule also requires that the Company should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

Customer identification requirements shall be as per the provisions of the said rule.

PERIODIC UPDATION OF KYC

As per the revised Master Direction on KYC dated 10th May 2021, the Company has adopted a risk-based approach for periodic updation of KYC in the following manner:

S.no	Basis Risk category Frequency	Basis Risk category Frequency
1	High risk customers	Once in every two years from the date of opening of the account / last KYC updation
2	Medium risk customers	Once in every eight years from the date of opening of the
3	Low risk customers	Once in every ten years from the date of opening of the account / last KYC updation

The company shall obtain self-declaration from Individual customers and non- Individual customers in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained 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.

The Company shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in clause 3 of this policy, for the purpose of proof of address, declared by the customer at the time of periodic updation.

In case of change in KYC information of a non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

MONITORING OF TRANSACTIONS AND MAINTENANCE OF RECORDS OF TRANSACTIONS

It is equally essential for the Company to have a clear knowledge and understanding about the normal working pattern and activity of the customer so that the Company can identify all such unusual transactions which would fall outside the normal transactions of the customer.

To achieve this purpose, ongoing monitoring is necessary. The extent of such monitoring will depend upon the level of risk involved in a particular account. Any transaction or activity of the customer which gives rise to suspicion will be given special attention. Such monitoring is important to keep a check on any act or omission of the customer which may amount to money laundering or support any act relating to use of finance for criminal activities.

SUSPICIOUS TRANSACTION REPORT (STR)

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted. Throughout this guideline, any mention of a "transaction" includes one that is either completed or attempted.

"Reasonable grounds to suspect" is determined by what is reasonable in the circumstances, including normal business practices and systems within the industry.

There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behavior.

Responsibility:

The Compliance Team in coordination with the senior management team should review the STR Reports framed by the compliance team, and finalize the transactions to be reported as STR. The principal officer is responsible for reporting the same to FIU-IND. The following activities will be

undertaken in the process of reporting suspicious transactions:

· Monitoring of large value and exceptional transactions based on alerts defined.
· Liaison with the senior management Team for responses / clarifications on STR alerts.
· Escalation of suspicious transactions to respective business heads / product heads.
· Filing Cash Transaction Report (CTR) with the FIU by 15th of subsequent month.
· Filing Suspicious Transaction Report (STR) with FIU by not later than seven working days on being satisfied that the transaction is suspicious.
· Scrutinizing samples of customer data against UNSCR and other negative lists as issued by NHB/ other Regulatory / Statutory entities from time-to-time and escalating the same to Business Heads.

The Company shall ensure the following:
· Carry out an internal Money Laundering and Terrorist Financing risk assessment periodically involving the below mentioned aspects in relation to the on-boarded clients
· 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.
· Cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time
·Be commensurate to the size, geographical presence, complexity of activities/structure, etc. of the clients
· Apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.

CASH TRANSACTION REPORTS (CTR)

All individual cash transactions in an account during a calendar month, computed separately, exceeding Rupees Ten Lakhs or its equivalent in foreign currency, during the month should be reported to FIU-IND. However, while filing CTR, details of individual cash transactions below Rupees Fifty Thousand may not be indicated.

The Principal Officer should ensure submission of CTR for every month to FIU-IND before 15th of the succeeding month. CTR should contain only the transactions carried out by the Company on behalf of their clients/customers excluding transactions between the internal accounts of the Company.

COUNTERFEIT CURRENCY REPORT (CCR)

A separate Counterfeit Currency Report should be filed for each incident of detection of Counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of a person, a separate CCR should be filed for each such incident. These transactions should be reported to the Director, Financial Intelligence Unit, India by not later than the 15th of the succeeding month from the date of occurrence of such transactions.

In the event any fake or counterfeit note is detected by branch staff, despite taking all precautions; then it must be noted in a cash register separately. Reporting of the case with full details like name of customer, amount, denomination, date - must be reported by branch manager to Compliance Department at HO with copy to senior management team members.

Compliance to collate all the data and report to RBI under PMLA, as mentioned above.

MONITORING & REPORTING OF TRANSACTIONS

The Company will keep a continuous vigil, if any of the following acts or events is noticed in relation to the customer's approach or behavior while dealing with the Company:

1. Reluctance of the customer to provide confirmation regarding his identity.

2. Loan money is used for a purpose other than the one mentioned in the sanction letter form and the real purpose is not disclosed to the Company.

3. Customer forecloses the loan prior to the stated maturity.

4. Customer suddenly pays a substantial amount towards partial repayment of the loan.

5. Customer defaults regularly and then pays substantial cash at periodical intervals i.e. once in six months.

The Company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose. The Company may prescribe threshold limits for a particular category of accounts and pay close attention to the transactions that exceed the prescribed threshold limits. Keeping this in view, the Company shall pay particular attention to the cash transactions which exceed the limits of Rs. 10 lakhs, either per transaction or credit and debit summation in a single month. This would include a transaction where the customer by way repayment of loan, whether in part or full, deposits Rs. 10 lakhs and above in cash. Such transactions shall be reported to the compliance department and the Principal Officer appointed as per this policy. In such cases, the Company shall keep a close and careful watch on the subsequent mode of payments adopted by such customers.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention of the Company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through that account. Company shall ensure that proper record of all transactions and cash transactions (repayments) of Rs.10 lakhs and above in the accounts is preserved and maintained as required under the PMLA.

The Company shall introduce a system of maintaining proper record of the following transactions:

i. All cash transactions of the value of more than rupees Ten lakhs to its equivalent in foreign currency;

ii. All series of cash transactions integrally connected to each other which have been valued below rupees Ten lakhs 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 lakhs;

iii. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;

iv. All suspicious transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of valuable security or a document has taken place facilitating the transactions;

v. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules

The Company shall ensure that it continues to maintain a proper record of all cash transactions (deposits and withdrawals) of Rs. 10 lakhs and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to the controlling / head office on a fortnightly basis.

The records shall be preserved in the following manner:

i) The nature of transactions
ii) The amount of the transaction and the currency in which it was denominated
iii) The date on which the transaction was conducted
iv) The parties to the transaction

The information in respect of the transactions referred to in clauses I, II and III referred above will be submitted to the Director - FIU every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause IV referred above will be furnished promptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.

The information in respect of the transactions referred to in clause V referred above will be furnished promptly by the Director - FIU in writing, or by fax or by electronic mail not later than seven working days on being satisfied that the transaction is suspicious.

Strict confidentiality will be maintained by the Company and its employees of the fact of furnishing / reporting details of such suspicious transactions.

As advised by the FIU-IND, New Delhi; the Company will not be required to submit 'NIL' reports in case there are no Cash / Suspicious Transactions, during a particular period.

The reporting of the requisite information in respect of cash transactions and suspicious transactions shall be as per the provided formats and shall be in accordance with the reporting guide provided by FIU-IND.

The required information will be furnished by the Company directly to the FIU-IND, through the designated Principal Officer.

High risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such high-risk accounts, taking note of the background of the customer, which will include country of origin, source of funds, the type of transactions involved (like accounts having unusual transactions, inconsistent turnover, etc.) and other risk factors. Additionally, the Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures on the basis of the revised risk categories.

In addition to the Ordinary Monitoring Standards, any high-risk accounts should also receive the following monitoring:

· Conduct periodic (at least quarterly) reviews of all medium to high-risk accounts

· Create additional reports designed to monitor all transactions in an account to detect patterns of potential illegal activities

· Follow up on any expectations detected from the monitoring reports by contacting the account owner personally to inquire about the unusual activity detected and regularly report status of account inquiries to the Compliance Officer. The Company shall monitor and report such transactions in a manner specified in "Annexure-D".

d.) Risk Management

The Board of Directors of RSFCPL 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 compliance department to ensure that RSFCPL's policies and procedures are implemented effectively.

RSFCPL's internal control and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function will provide an independent evaluation of RSFCPL's policies and procedures, including legal and regulatory requirements. RSFCPL will ensure that its internal control systems and machinery is staffed adequately with individuals who are well-versed in such policies and procedures or hire the services of a reputed Company engaged in providing quality services in the said field. They will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Board at quarterly intervals.

RSFCPL will have an ongoing (at regular intervals) employee training program so that members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers.

10. Appointment Of Principal Officer (Po)

As required under the Prevention of Money Laundering Act, 2002 (PMLA), a senior official will be appointed as the Principal Officer of our Company. The Principal Officer shall *inter alia* be responsible for effective communication and liaison with RBI and other enforcement agencies and Roles and responsibilities of the Principal Officer would also include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and fulfil obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time.

The name, designation and address of the principal Officer will be communicated to FIU-IND.

The Board in its meeting held on October 16, 2021 has duly appointed the below mentioned person as "Principal Officer", who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations:

Name	PRATHAP REDDY EAMANI
Designation	Director
Address	D No New 5D (Old No. 4D) Rajaram Film Directors Colony Kodambakkam Chennai TN 600024 IN
Contact Details	9989078797

11. Appointment Of Designated Director

As required by Prevention of Money Laundering Act, 2002 (PMLA) and Reserve Bank Circular vide DNBR (PD)CC. No. 005 /03.10.42/2014-15 dated December 1, 2014, A director or Managing director or whole-time director will be appointed as Designated Director for ensuring compliance with the obligations under the PML Act.

The name, designation and address of the Designated Director shall be communicated to FIU-IND.

The Board of directors in their meeting held on November 16, 2021 has appointed the below mentioned person as the "Designated Director" and the same has been duly communicated to FIU:

Name	B. Venkata Ramana
Designation	Director
Address	D No New 5D (Old No. 4D) Rajaram Film Directors Colony Kodambakkam Chennai TN 600024 IN
Contact Details	9550644412

12. Money Laundering and Terrorist Financing Risk Assessment

a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should 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, REs shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

b. The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the company Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in

alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

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

13. Identification of Beneficial Ownership

The organization should determine the beneficial ownership and controlling interest in case of applicants who are not individuals and the KYC of the beneficial owners should be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice.

S. No.	Applicable	Guidelines	
i)	Where the client 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 a controlling ownership interest or who exercises control through other means	a. Ownership of/entitlement to more than 25 % of shares or capital or profits of the company b. Control shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of them shareholding or management rights or shareholders agreements or voting agreements
ii)	Where the client is a partnership firm or a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person	Ownership of/entitlement to more than 15% of the capital or protiofate partnership.
iii)	Where no natural person is identified under (i) or (ii) above	The beneficial owner is the relevant natural person who holds the position of senior managing official	

There are certain indicative guidelines issued by RBI from time to time for customer identification requirements with regard to matters, such as Trust / Nominee or Fiduciary Accounts, Accounts of companies & firms, Client Accounts opened by professional intermediaries, Accounts of Politically Exposed Persons resident outside India and Accounts of non-face-to-face customers and these guidelines should be adhered to the extent applicable.

14. Record Retention

Records pertaining to identification of the customer and his address obtained while opening his account and during course of business relationship should be preserved accordance with the section 12 of the PMLA Act 2002 which specifies for at least five years after the business relationship has ended in case of all transaction related to the individuals or for at least five years from the date of transaction between a client and the reporting entity in case of evidencing identity of its clients and beneficial owners.

15. Reporting to Central KYC Registry (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities (LE)' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

The customer information related to LEs (Legal Entities) should be submitted to CKYCR for accounts of LEs (Legal Entities) opened on or after commencement of NBFI business activities.

Further, during periodic updation, customers' KYC details are to be migrated to current Customer Due Diligence (CDD) standards.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and customer is not required to submit any KYC records unless

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

KYC Identifier generated by CKYCR, should be communicated to the Individual/LE.

16. Reporting Requirements to Financial Intelligence Unit – India.

RSFCPL shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

The reporting formats and comprehensive reporting format guide prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic

utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of RSFCPL, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIUIND on its website http://fiuindia.gov.in.

- 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 Rule shall be constituted as a separate violation. RSFCPL shall not put any restriction on operations in the accounts where an STR has been filed. RSFCPL shall keep the furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

- However, Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put into use as a part of effective identification and reporting of suspicious transactions.

17. Reporting Requirement under Foreign Account Tax Compliance Act (FATCA).

Under FATCA and CRS, RSFCPL shall take steps for complying with the reporting requirements:

1. Registration to be done on the URL https://incometaxindiaefiling.gov.in for filing the returns.
2. Submit e-filing report by using digital signature of the designated director either uploading form 61B or NIL report.
3. Reference can be taken from www.fedai.org.in/revaluationrate.aspx for carrying out due diligence procedure for the purpose of identifying reportable accounts under section 114H of Income Tax Account.
4. Help of IT framework for due diligence, for recording and maintaining the information.
5. The Senior Management constituted under this policy will ensure compliance.

Annexures –A

Customer Identification Process

Every employee of RSFCPL or RSFCPL representative as specified in respective product policies such as Dealer or DSA shall establish a customer relationship only after the identity and address of the customer and all those who represent the customer has been verified and found satisfactory.

Step 1

The process of customer acceptance begins with meeting/interaction with the customer.

Step 2

The customer is required to complete the Application Form wherein details on the background and facilities opted by the customer are recorded. All applicable fields should be completed. (Not applicable fields should be marked as "NA")

Step 3

The details furnished in the Application Form shall be supported by Photograph (applicable in case of individual) Proof of Identity,

Proof of Address and Relationship Proof. The documents that can be accepted to support the identity, address and signature of all parties signing the agreement i.e., applicant, co- applicant, guarantor and Ultimate beneficial owner (UBO) are listed in the attached **Annexure-C provides List of Important Instructions, Documents Accepted as Proof of Identity, Proof of Address, and Relationship Proof (as applicable)**.

The customer should sign across the photograph and should sign on all the photocopies of the KYC Documents Identity and address proof documents are collected to identify the customers and confirm their stay at a particular address with the help of reliable, independent source documents, data or information. Photograph should be a recent color passport size photograph.

Step 4

The photocopies of supporting documents obtained as Proof of Identity and Proof of Address and relationship proof should be verified with originals and certified by the person verifying the same as 'True Copy' i.e., Original, Seen and Verified (OSV). The RSFCPL Employee or RSFCPL Representative who meets the customer should perform the verification. (OSV stamp with name, signature and employee/representative code).

Step 5

The Internal Deduplication Check (Internal Deduplication) and Credit Bureau Check should be conducted. Necessary de-duplication check to be done before opening a new account as well as check to be done to ensure as far as possible that the identity of the applicant does not match with any person with known criminal background or with the willful defaulters as per the list published by the RBI or with banned entities such as individual terrorists or terrorist organizations or list of

individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) etc. Deduplication Check (Internal Dedup) and Credit Bureau Check should be mandatorily done on the basis of the ID number mentioned on the valid KYC document as mentioned in Annexure A1.

Step 6

Verification of customer information (which includes Tele-verification) should be conducted by RSFCPL employee or RSFCPL representative.

RCU checks are primarily done on the pre-sanction documents submitted by the customer/applicant to verify the authenticity of documents submitted.

It must be noted that FI checks, Tele-verification checks and fraud checks are only in the nature of confirmation of the customer's contact details for deriving comfort on such cases and such FI and TVR cannot act as a substitute for KYC documents.

Step 7

The welcome letter should be sent to the customer within 21 working days from the date of inception of contract.

Annexure-B

Indicative list for risk categorization

Low Risk Customers

All other customers (other than High and Medium Risk category) whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

- Well governed corporates
- Salaried employees having definite and well-defined salary structure,
- Employees of Government Departments or Government owned companies,
- Statutory bodies,
- Self-employed individuals, however with regular income and good credit behavior

Medium Risk Customers

- Stock brokerage
- Import / Export- Gas Station
- Car / Boat / Plane Dealership
- Electronics (wholesale)
- Travel agency
- Telemarketers
- Providers of telecommunications service, internet café, International direct dialing (IDD) call service.
- Dot-com company or internet business
- Pawnshops
- Auctioneers
- Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
- Sole Practitioners or Law Firms (small, little known)
- Notaries (small, little known)
- Secretarial Firms (small, little known)
- Accountants (small, little-known firms)
- Venture capital companies

High Risk Customers

- Foreign Delegates or those working in Foreign High commissions or Embassies,
- Senior Politicians,
- Senior Judicial Officers,
- Senior Military Officers,
- Senior Executives of State-Owned Corporations and
- Officials of important and leading political parties
- Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the

location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;

- Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner
- Non-face-to-face customers
- High net worth individuals
- Firms with 'sleeping partners
- Companies having close family shareholding or beneficial ownership.
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff does not constitute physical presence;
- Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the Company;
- Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.;
- Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;
- Gambling/gaming including "Junket Operators" arranging gambling tours;
- Jewellers and Bullion Dealers; - Dealers in high value or precious goods (e.g., gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
- Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
- Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
- Customers that may appear to be multi-level marketing companies etc.

Additional indicative list of High-Risk Customers:

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 & 1988 [2011] linked to Al Qaida & Taliban etc.;
- Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
- Individuals and entities in watch lists issued by Interpol and other similar international organizations; - Customers with dubious reputation as per public information available or commercially available watch lists;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- Customers based in high-risk countries/jurisdictions or locations as identified by FATF from time to time.
- Individual, who is a prisoner in jail.
- Accounts of Embassies / Consulates.
- Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low-level staff does not constitute physical presence.
- Investment Management / Money Management Company/Personal Investment Company.
- Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)

Annexure-C

List of KYC documents for different type of customers

Features	Documents
Accounts of individuals - Legal name and any other names used - Correct permanent address	(i) Passport (ii) Voter's Identity Card (iii) Driving license (v) proof of possession of Aadhaar number (iv) Job card issued by NREGA duly signed by an officer of the State Government (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank.
	For Address (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) (any one document which provides customer information to the satisfaction of the bank will suffice)
Accounts of companies	
- Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Permanent Account Number of the company Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account one copy of an officially valid document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
Accounts of partnership firms	
- Legal name - Address - Names of all partners and their addresses -Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Permanent Account Number of the partnership firm; and (iv) one copy of an officially valid document containing details of identity and address, one recent photograph and Permanent Account Number or Form No.60 of the person holding an attorney to transact on its behalf."; (v) Telephone bill in the name of

	firm / partners (optional) (vi) Any other prescribed equivalent e-documents
Accounts of Proprietary Concerns	
-Name, Address and Activity of the Proprietary Concern.	Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/license issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate/ registration document issued by Sales Tax / Service Tax / Professional Tax authorities, License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. RSFCPL may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account. The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.
Trust/Association/Society/Club - Registered - Legal name - Address - Names of all trustee/members settler, and beneficiary and their addresses	One certified copy of each of the following documents shall be obtained: 1. Registration Certificate. 2. Certified "True and updated" copy of Trust Deed / Bye Laws / MOA attested by Secretary/ Managing Trustee/ Chairperson.

-Telephone numbers of the trust/AOP/Club and all trustee /members, settler and beneficiary.	3. Certified " True and Updated" Copy of Certificate of Registration (For Club / Society / Association/ Trust) signed by the secretary. 4. List of all Office Bearers / Trustees, along with Settlers (including any person settling assets into the Trust), grantors, protectors, beneficiaries (when they are defined) and in case of Foundations the founders / managers / directors, to be obtained on the letterhead with their addresses. 5. Certified copy of Resolution to borrow facility / loan signed by managing trustee/chairperson/ secretary. 6. OVD of Trustee, UBO and authorized signatory signing the facility / loan documents as specified in "Individuals" Section above. 7. Notarized Power of Attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract, on behalf of the firm. Certified copy of OVD of PoA holder has to be obtained. Notarized PoA would not be required if one or more members of the Trust/Society/etc. are directly executing the contract. (Annexure B4). 8. Information to be collected about the shareholding/ownership 9. share/profit share/beneficiary for establishing percentage holding.
Hindu Undivided Family (HUF) - Legal name - Address - Names of karta and all members and their addresses -Telephone numbers of the HUF and karta and all members.	One certified copy of each of the following documents shall be obtained: 1. HUF letter with specimen signatures of the Karta and all adult co-parceners as per HUF Declaration Format provided in Annexure B1. 2. PAN Card in the name of HUF. 3. OVD of Karta. (As applicable for Individuals) 4.Address proof of the HUF: a. Latest available Income Assessment order OR b. Bank statement of account with existing Banker (Scheduled Bank) bearing the account holder's address with entries of preceding 3 calendar months from the date of Log in.

Unregistered Association/Body of Individual, Unregistered trusts, Unregistered Partnership firm - Legal name - Address - Names of all partners/Members and their addresses -Telephone numbers of the firm/AOP/BOI and their Members and partners	1. Partnership Authority Letter (PAL): All pages of the Partnership letter to be signed by minimum one partner. All Partners should sign and authenticate at least the last page of the PAL under rubber seal (for capacity). The PAL should be on the Firm's Letterhead. Any alterations on any page to be signed by all the partners. Certified copy of OVD in respect of the person holding a PAL to transact on its behalf. 2. Notarized Power of Attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract, on behalf of the firm. Certified copy of OVD of PoA holder has to be obtained. Notarized PoA would not be required if one or more partners The firm is directly executing the contract. (Annexure B4). **1.** Proof of legal existence of such entity in the form of PAN Card/ /Service Tax/VAT/Sales Tax Registration/ CST/VAT/GST certificate/ Certificate of registration document issued by Sales Tax/Service Tax/Professional Tax authorities. 4. Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding.

List of important instructions pertaining to documents specified in KYC Documentation

- The KYC requirement will be applicable for Applicant, Co-Applicant, Guarantor, UBO Including Business Partners.
- Copies of the OVD and Relationship proof should be verified with originals and certified by the person verifying the same as 'True Copy' i.e., Original, Seen and Verified (OSV). The RSFCPL Employee or RSFCPL Representative who meets the customer should perform the verification (OSV stamp with name, signature and employee / representative code).
- Each of the KYC (OVD, Photograph and Relationship Proof) documents obtained from customers should be self - certified by all types of customers.
- OVD of Ultimate Beneficial Owner (UBO) has to be mandatorily collected.
- OVD issued in incomplete names (only personal names (first names) as in the case of Voter ID in certain states) cannot be accepted.
- OVD should contain the complete address as captured in the application form. If there is any difference or if incomplete another document containing the address as per application form should be asked for from the applicant.

- Marriage Certificate issued by state govt. or gazette notification to be used in case of name change along with certified copy of OVD in existing name to be obtained for identity and address proof of the person and can be used for relationship proof.
- In case of a partnership between individual(s) and entity(s) or between entity(s), the KYC requirements for such entity(s) also need to be complied with in addition to the KYC requirements of the partnership. Partnership firm, HUF & Private limited firm cannot become partners in any partnership firm.

Address Proof – For customer identification, the following norms to be ensured:

- The customers shall be required to furnish separate proof of address for permanent and current addresses, if these are different.
- In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/his local address on which all correspondence will be made by the RSFCPL.
- The local address for correspondence, for which their proof of address is not available, shall be verified through positive confirmation through personal visit.
- In case it is observed that the address mentioned as per 'proof of addresses has undergone a change, team shall ensure that fresh proof of address is obtained within a period of six months.

Re-Use of OVD for KYC– If the same customer comes for repeat funding within a period of six months from last Loan Application date, then collection of fresh OVD is not mandatory, provided:

- Last file was KYC compliant (Physical file and scanned copies in DMS) and the address mentioned in Application Form for proposed funding matches with the downloaded OVD and A declaration shall be provided by RSFCPL Employee that the OVD has been downloaded from DMS. The employee downloading the document shall sign all OVD mentioning name, employee id, date and
- If the OVD has been pre-written by a customer for restricted use, then fresh OVD would be required to be collected.
- In case Field Investigation / customer interaction reports that customer address does not match with the downloaded OVD then fresh OVD shall be obtained.

ANNEXURE-D

Process for monitoring and reporting of suspicious transactions

1. Raising suspicion

When the concerned officer has reason to believe that a transaction is/ may be a suspicious transaction, which may be linked with terrorist activity or money laundering, s/he must flag the issue forthwith to the senior management. The concerned officer may consider the following for the purpose of flagging such issue:

· Amount involved are related to crimes of money laundering, the financing of terrorism, or the financing of illegal organizations;
· Amount involved are intended to be used in an activity related to such crimes.

2. Identification and evaluation

Once the issue is flagged, a formal due diligence is to be conducted to evaluate the suspicion, which shall factor all the attributes and nature of the transaction and in terms of volume, track record, time of transaction, KYC records, behavioral patterns, customer due-diligence information etc.

Additional details in relation to a client can be obtained to substantiate further information. Once proper documentation is obtained and if the concerned officer is satisfied, the issue shall be closed and recorded.

Mere presence of an indicator of suspicion does not necessarily always mean that a transaction is suspicious and needs to be reported. When determining whether a transaction is suspicious, consideration is given to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its due diligence profile. In some cases, patterns of activity or behavior that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another.

In case, the concerned officer is not satisfied, it shall be further evaluated, and a formal report shall be submitted to senior management.

3. Reporting of STR

The senior management may record the reasons therein and evaluate on onward reporting to FIU-IND. Once the senior management is satisfied that the suspicious transaction is valid and reportable, the same is reported to FIU-IND in accordance with the prescribed formats.

The fact of furnishing of suspicious transactions shall be strictly kept confidential to ensure that there is no tipping off to the customer at any level.

Annexure-E

BUSINESS PARTNER DUE DILIGENCE PROCEDURE

Definition

A Business Partner is defined as "any party who establishes relationships on behalf of their clients with RSFCPL and parties whose employees have access to RSFCPL's data and or systems (outsourcing partners, providers of administrative / IT services, External auditors, data entry operators, Consultancy firms etc.)" The Outsourcing Policy of RSFCPL governs all Business Partner relationships.

KYC Policy including Risk Categorization will be applicable to all Business Partners including associates/agencies/intermediaries etc.:

Empaneled Lawyers - Empaneled Valuers - Vendors providing services like Selling Agents, Direct selling team / agents, Collection Agencies, Verification Agencies, Bidders etc. –
Any other intermediary.

RSFCPL will collect all KYC documents as specified in Annexures.

Due- diligence of Business Partners:

The Business Partner relationships are entered into at the Corporate Office /Regional Office/Head office level. Hence the Heads of Business Units/Departments are responsible to ensure adequate due diligence measures are applied before accepting a business partner. Following procedure to be followed:

Step 1

Heads of Business Units/Departments should collect information of the following parties as part of the due diligence:

(i) The Business Partner as a person as defined above.
(ii) Individuals who are authorized to act on behalf of the business partner.
(iii) The ultimate beneficial owner of the business partner,

Step 2

The Heads of Business Units/Departments should screen the names and date of birth/other relevant date of the Business Partner and its UBO/Representatives against the freeze /negative lists / Dedup database. In case of hits on the lists screened, enhanced measures should be applied to ascertain the identity of the Business Partner. The enhanced measures are the same as the enhanced measures for Customer Acceptance.

Step 3

A pre-employment screening of the staff of the business partners who have /may have access to RSFCPL's data or systems should be Performed.

Review of Business Partners:

Periodicity

The Business Partner files have to be reviewed with every material change that comes to the notice of RSFCPL. Records of business partners should be reviewed every year.

Step 1

The Business / Department that has performed the due diligence on accepting the Business Partner is also responsible for periodical review. **The Audit department shall monitor and ensure all the Business / Department comply with this procedure and perform timely reviews**.

Step 2

The review should be performed using the due diligence form for Business Partners. The revised due diligence forms should be kept along with the Agreement.

Any clarification with respect to meaning and interpretation of the norms specified in this note can be issued by the Chief Risk Officer within the gamut of applicable RBI master circular of KYC and AML.

Note:

ನೀವುಕನ್ನಡದಲ್ಲಿಈಡಾಕಯುಮೆಂಟ್ಅನ್ಯನಹೆೇಂದಲಯಬಯಸಿದರೆ, ದಯವಿಟ್ಯು director@rsecuredfinance.com ನಿ್ಲನ್ಮೆಂದಿಗೆಸೆಂಪಕಕದಲ್ಲಿರಿ. 7 ಕೆಲಸದದಿನ್ಗಳಒಳಗೆನಮಗೆಡಾಕಯುಮೆಂಟ್ಕನ್ನಡದಲ್ಲಿಲಭ್ಾವಾಗಯತ್ತದೆ

മലയാളംഭാഷയിൽഈപ്രമാണംലഭിക്കണമെന്നുണ്ടെങ്കില്, ദയവായി director@rsecuredfinance.com എന്നവിലാസത്തില്ഞങ്ങളുമായിബന്ധമെടുക. 7 പ്രവർത്തിദിവസങ്ങൾക്കുള്ളിൽഇത്നിങ്ങൾക്ലന്താഷന്ത്താമടലഭയമാക്കും

ಮೀರುಈಪತ್ರಾನ್ನಿತೆಲುಗುಲೆಪೊಂದಾಲನುಕೊಂಟೆ, ದಯಚೆೇಸಿ director@rsecuredfinance.com ಕಮೆಯಿಲ್ಪೆಂಪೊಂಡಿ. ಮೆಮು 7 ಪನ್ನರೆಜುಲಲೆತೆಂದುಬಾಟುಲೆಡೆಂಚುತ್ರಮು.

உங்களுடையஆவணங்கடைதமிழில்ததரிந்துதகொள்ை, எங்களின்மின்னஞ்சல்மூலமொகவும்ததொைர்புதகொள்ைலொம் director@rsecuredfinance.com வொரத்தில் 7 நொட்களும்உங்களுக்குஉதவுவதில்நொங்கள்மகிழ்ச்சிஅடைகிறொம்.

আপনিযনিএইনিব্যাংলাতেচাি্েতবআমাতিরসাতি director@rsecuredfinance.com এযযাগাতযাগকরুি।আমরা 7 কাযযনিবতসরমতযেএটিআপিারকাতেউপলব্ধকরতেযপতরখুনিহব।

ଯଦିଆପଣଏହିପ୍ରଲେଖଓଡିଆଭାଷାଲେଚାହାନ୍ତିଲେଲେଆମକୁdirector@rsecuredfinance.com ଲେଲଯାଗାଲଯାଗକେନ୍ତୁ। ଆଲମଖୁସି୍ଏହି୍ଏହିପ୍ରଲେଖଆପଣଙ୍କୁଓଡିଆଭାଷାଲେଏକସପ୍ତାହମଧ୍ୟଲେଉପେବ୍ଧକଲେଛୁ

యదిఆపుదిఅసమీయాతప్రలేఖదిచాలేతతలేఖ్రిగ్రహకదేఆమా్ేగతసంలయాగేక్షాకేక director@rsecuredfinance.com ఆదమఆలపాి్ాకఁదిి్ేి్ాలిసహాయకదేసుఖీహమ।

जरतुम्हालामराठीमध्येहाकागदपत्रहवाअसेलतरकृपयाआमच्याशीसंपककसाधा director@rsecuredfinance.com
वर. 7 ददवसांच्याआतआपल्यालातेउपलब्धकरुनदेण्यातआम्हालाआनंदहोईल.

જોતમારેઆડોક્યમુન્ેટગજુરાતીભાષામાાંજોઈતોહોયતોકૃપાકરી director@rsecuredfinance.com
ખાતેઅમારોસાંપકકકરો. તમનેકામકાજના 7 દિવસમાાંઉપલબ્ધકરાવીશ.