ORIX Leasing & Financial Services India Limited (OLFS)

"Know Your Customer" (KYC) & Anti Money Laundering (AML) Policy

A. PREAMBLE:

The KYC & AML Policy is devised basis the Reserve Bank of India (RBI) Master Direction no. RBI/DBR/2015-16/18 DBR.AML.BC. No.81/14.01.001/2015-16 ("KYC Directions, 2016"), amended from time to time and the ORIX Group Anti-Money Laundering (AML) Policy so as to follow certain Customer identification procedure while undertaking a Transaction either by establishing and account-based relationship or otherwise and to set standard for detection, prevention and management of money laundering, terrorist financing and sanctions risks by the Company. If applicable laws and regulations prohibit implementation of this policy, the same will be brought to the notice of the Reserve Bank of India.

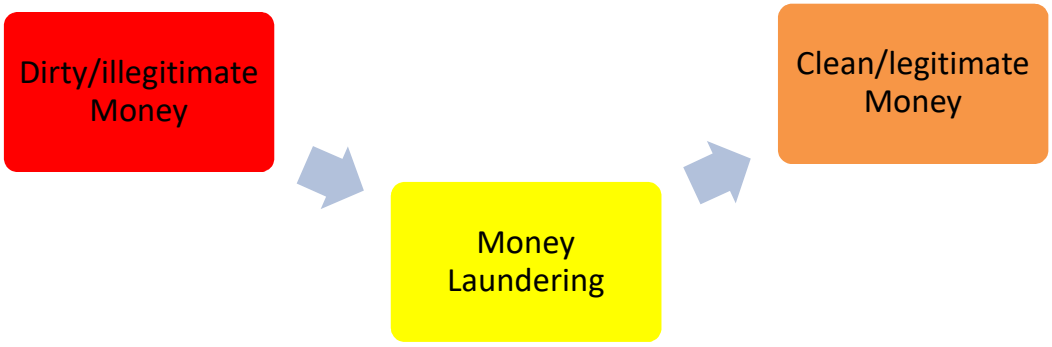
Accordingly, this KYC & AML Policy have been adopted by the Board suitably superseding the existing KYC and PMLA Policy of ORIX Leasing & Financial Services India Limited ('the Company/OLFS'), as amended from time to time.

B. BASIC BACKGROUND:

I. What is Money Laundering?

Money laundering may be generally described as the process by which the proceeds of illegal activities or funds from illegitimate sources are disguised in a manner that makes the proceeds appear to come from legitimate sources or activities. Although frequently equated with drug trafficking, money laundering can arise in many circumstances, including governmental corruption, financial fraud, tax evasion, proceeds of crime, hacking and other cyber-crimes, illegal trafficking of arms, illegal trafficking of minerals, precious metals or gems, exchange or export control violations and gambling etc. A related concern is terrorist financing, which may be generally described as a financial crime that uses funds to support the agenda, cause or activities of a terrorist organization. In the case of terrorist financing, funds may be raised both from legitimate sources (such as charitable organizations) as well as from criminal sources.

Money laundering activities take many forms and new methods arise regularly as those seeking to launder money engage in increasingly complex and creative schemes to avoid detection. Hence, it is critical that the Company exercise due caution in their daily business.



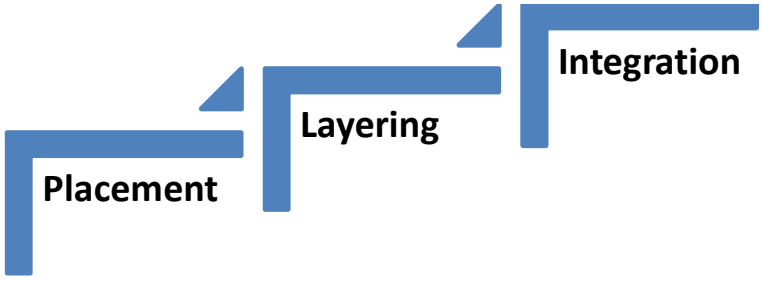
In simple terms money laundering is most often described as the "turning of dirty or black money into clean or white money". If undertaken successfully, money laundering allows criminals to legitimize "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of their income.

Section 3 of the Prevention of Money-Laundering Act, 2002 defines money laundering in following words:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

II. Money laundering cycle

Generally, money laundering encompasses a three-step process: placement, layering and integration. To be successful, the party seeking to launder money makes every attempt to avoid a "paper trail" to connect the three steps together. We should keep in mind that the use of the following "three step process" is on the rise in financial institutions since these entities offer a variety of services and instruments that can be used to conceal the source of funds associated with money laundering. Multiple financial institutions are often engaged to aid in such concealment:



(1) **Placement**: This involves the physical movement of the cash proceeds. For most criminal Transactions, cash is the most common medium of exchange and criminals who accumulate large volumes of cash are the most vulnerable to detection and seizure. As a result, money launderers will attempt, through placement, to channel the funds i.e. cash or cash-like instruments such as money orders or travellers checks into a bank.

(2) **Layering**: After the funds enter a bank, the money launderer will further separate the illicit proceeds from their illegal source through a process of layering. Layering occurs by conducting multiple, complex, financial transactions that make it difficult to link the money to an illegal activity i.e. efforts carried out by money launders to

disperse the funds and give them an air of legitimacy. This can involve moving funds into different accounts/contracts in different locations (e.g., illegal proceeds used to open up the bank account are wired out to fund the acquisition of property or securities). Layering disguises or eliminates the audit trail.

(3) **Integration**: During this process the money launderer will integrate the illicit funds into the economy by providing what appears to be a legitimate explanation for his or her illicit financial wealth. For example, integration of these proceeds might include the purchase of real estate, businesses, securities, automobiles or jewellery. Integration moves the funds back into the economy with the appearance of being normal business earnings. It would become extremely difficult at this point to distinguish between illicit funds and legitimate funds.

III. Money laundering risks:

The Company will be exposed to several risks, as stated below, if an appropriate KYC & AML framework is not established:

(1) **Reputation Risk** - Risk of loss due to severe impact on Company's reputation. This may be of particular concern given the nature of the Company's business, which requires maintaining the confidence of Customers.

(2) **Compliance Risk** - Risk of loss due to failure of compliance with key Regulations governing the Company's operations.

(3) **Operations Risk** - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

(4) **Legal Risk** - Risk due to any of the above risk or combination thereof resulting into the failure to comply with Act and RBI guidelines and having a negative legal impact on the Company. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

(5) **Financial Risk** - Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Company. Example of Financial Risk could be penalties imposed by the regulators in case of non-compliance of provisions of the Act and RBI guidelines.

C. OBJECTIVES OF THE POLICY:

Integrity is of utmost importance within the Company and ORIX Group (ORIX Group means 'ORIX Corporation, Japan', the ultimate holding Company and its subsidiaries). The guiding principle is that the Company only seeks to do business with Customers that do not pose unacceptable money laundering, terrorist financing and sanctions risks for the Company and will not implicate the Company in Transactions involving criminally derived proceeds or being used, intentionally or unintentionally, directly or indirectly by any unsocial elements for money laundering activities or terrorist financing activities or Transaction with sanctioned

parties. The Company will implement group-wide programmes against money laundering and terror financing, sharing information required for the purposes of Customer's Due Diligence (*as defined below*) and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

The objective of this Policy is broadly to:

(1) Issue a statement of policies and procedures, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;

(2) Ensure that the content of this Policy is understood by all employees;

(3) To establish a framework for adopting appropriate KYC & AML procedures and controls in the operations/business processes of the Company and regularly review the policies and procedures on Customer identification & on prevention of money laundering and terrorist financing to ensure their effectiveness;

(4) Adopt Customer acceptance policies and procedures which are sensitive to the identity risk of Customers & risk of money laundering and terrorist financing;

(5) Educate and sensitize the concerned work group within the organization and the Customers about the objectives of KYC & AML framework and of the requirements, to be complied with, emanating therefrom;

(6) To prevent the Company's business channels/products/services from being used as a channel for money laundering;

(7) To ensure compliance with the laws and regulations in force from time to time;

(8) To protect the Company's reputation; and

(9) To assist law enforcement agencies in their effort to investigate and track money launderers.

D. DEFINITIONS:

For the purpose of this Policy,

(1) "**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.

(2) **"Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);[1]

[1] "Aadhaar number" means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section.

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

(4) **"Beneficial Owner (BO)"** is any natural person(s) who ultimately owns or controls the Customer and /or the natural person(s) on whose behalf a Transaction or activity with the Company is being conducted. A list of persons who are to be considered as such BOs in relation to a Customer is given below:

(a) Where the **Customer is a company**, the Beneficial Owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.

(ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

(iii) Where the Customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) Where the **Customer is a partnership firm**, the Beneficial Owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.

Note: For the purpose of this sub-clause, "Control" shall include the right to control the management or policy decision.

(c) Where the **Customer is an unincorporated association or body of individuals**, the Beneficial Owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

---

[2] "authentication" 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 for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the Beneficial Owner is the relevant natural person who holds the position of senior managing official.

(d) Where the Customer is a **trust**, the identification of Beneficial Owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(5) **"Certified Copy"** Obtaining a certified copy by the Company will mean comparing the copy of the proof of possession of Aadhaar number where Offline Verification cannot be carried out or officially valid document so produced by the Customer with the original and recording the same on the copy by the authorized officer.

(6) "**Customer**" in the context of the diverse businesses within the Company will broadly include who is engaged in a Transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the Transaction or activity, is acting and depending on the nature of the Company's business may include, without limitation: (i) any Obligor(s) or (ii) any entity in which the Company wants to make an investment.

(7) **"Customer Due Diligence (CDD)"** means identifying and verifying the Customer and the Beneficial Owner using reliable and independent sources of identification.

(8) **"Customer Identification"** means undertaking the process of CDD.

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

(10) "**Designated Director**" means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and shall be nominated by the Board.

(11) "**Digital KYC**" means the capturing live photo of the Customer and OVD, where Offline Verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act.

(12) "**Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000) (IT Act).[3]

[3] Clause (p) of subsection (1) of Section 2 of IT Act defines ''Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of IT Act

(13) "**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.

(14) **"Group"** The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961)[4].

(15) **"High Risk Countries"** are those countries which are prone to sanction & money laundering risks and lists of such countries are periodically advised by ORIX Corporation to ORIX India Group.

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

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

(18) "**Obligor**" includes a person or entity that, as a lessee including Co-lessee, borrower including Co-borrower, guarantor, counter party or otherwise, is obligated to the Company pursuant to Transaction with the Company.

(19) "**Officially Valid Document (OVD)**" shall mean identification documents of Customer [also referred to as '**Know Your Customer (KYC)**' documents] and / or Third Party Agent such as residential address of an Individual or registered address of non-individual and their respective identity, which is issued by government authorities or municipal corporations, as the case may be, which are more specifically listed in **Exhibit 1 to this Policy**.

(20) **"Offline Verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016)[5]

(21) "**Ongoing Due Diligence**" means regular monitoring of Transactions in accounts to ensure that they are consistent with the Customers, Customers' business and risk profile and source of funds/wealth.

---

[4] "group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes:
(i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or
(ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

[5] "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.

(22) **"Politically Exposed Person (PEP)**" 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.

(23) "**Periodic Updation**" means step taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI.

(24) "**Principal Officer**" means an officer, at the management level, nominated by the Company, responsible for ensuring compliance, monitoring transactions and sharing and reporting information as required under the Rules.

(25) "**Red flag**" refers to a fact, event, or set of circumstances, or other information that may indicate a potential legal compliance concern for illegal or unethical business conduct. When conducting due diligence of Customers, "Red flags" should trigger concern for further analysis. Indicative Red flags for the purpose of this Policy are defined in the Exhibit 11

(26) **"Sanctions Lists**" means the list which are approved by and periodically circulated by the United Nations Security Council (UNSC) and also the lists as specified in Clause F(IV)(1) below consisting of name of individuals/entities (Non individual), suspected of having terrorist links.

(27) "**Suspicious Transaction**" in terms of Rule 2(1)(g) of Rules, Suspicious Transaction means a Transaction, whether or not made in cash, which, to a person acting in good faith:

(a) Gives rise to a reasonable ground of suspicion that it may involve the proceeds of offence specified in the Schedule to the Act, regardless of the value involved; or
(b) Appears to be made in circumstances of unusual or unjustified complexity;
(c) Appears to have no economic rationale or *bona-fide* purpose; or
(d) Give rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
(e) Large and complex Transactions including RTGS Transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the Customer, which have no apparent economic rationale or legitimate purpose needs to be mandatorily monitored and appropriate actions, (if any) such as reclassification of Risk Rating and / or reporting to FIU should be done

Indicative list of Suspicious Transactions is specified in **Exhibit 11**

(28) "**Third Party Agents (TPA)**" means any person or entity from whom either any services are outsourced or goods are procured.

(29) **"Transaction"** means any financial transaction carried out or sought to be carried out with Customer or with TPA post onboarding such Customer or TPA.

(30) **"Walk-in Customer"** means a person who does not have an account-based relationship with the Company but undertakes Transactions with the Company.

E. KEY ELEMENTS OF THIS POLICY:

I. Customer Acceptance Criteria / Policy

Without prejudice to the generality of the aspect, the Customer Acceptance criteria / Policy of the Company will be as under:

(1) No account is opened in anonymous or fictitious/*benami* name. Permanent Account Number (PAN) copy (certified true copy) shall have to be obtained mandatorily from all Customer(s) In exceptional cases where PAN is not available with Customer, FORM 60 as prescribed under Income Tax Act, 1961 and Rules framed there under needs to be obtained.

(2) PAN shall have to be verified from the verification facility of the issuing authority.

(3) The certified true copy of GST Certificate shall have to be obtained to the extent (if applicable) and the GST number shall have to be verified from the search/verification facility of the issuing authority.

(4) Obtain OVD documents from Customer and also TPA as specified in Exhibit 1 depending on category of Customer or TPA, as the case may be.

(5) In case in person meeting with the Obligor, either the Obligor should visit office/ branch of the Company or concerned official should visit the Obligor at his residence or office address to get desire comfort on identity of Obligor and get necessary documents filled in and signed.

In case of Digital KYC, the process to be followed is specified in **Exhibit 2**

(6) No account is opened and/or Transaction is carried out without following CDD Process As specified in Section II (4) below. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the Customer or non-reliability of the documents/information furnished by the Customer. The Company will file STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the Customer.

(7) Any additional information, which is not specified in this Policy, is obtained only on need basis that to with the explicit consent of the Customer.

(8) CDD Procedure is followed for all the joint account holders / Co-applicants / Guarantors, while opening a joint account.

(9) Any other person can act on behalf of the Customer only after obtaining mandate from the Customer.

(10) The KYC information / documents are sought from Customer so as to ascertain and verify identity of Customer while opening an account or establishing account-based relationship with Customer and during the Periodic Updation.

(11) A Unique Customer Identification Code (UCIC) will be allotted while entering new relationships with Customer as also the existing Customers by the Company. Each Customer should have only one UCIC.

(12) The Company will apply the CDD Process at the UCIC level. Thus, if an existing KYC compliant Customer of the Company desires to transact with different business vertical, there shall be no need for a fresh CDD exercise provided 1 year has not elapsed from the date of allotment of UCIC.

***Note**:*

CDD exercise shall also not be necessary where the Customer of holding company of the Company, i.e., ORIX Auto Infrastructure Services Limited (OAIS) is required to be on boarded as a Customer of the Company provided:

(a) *One year has not elapsed from carrying out CDD exercise by OAIS;*

and

(b) *the CDD process of OAIS is similar to CDD process of the Company.*

(13) Suitable system is put in place to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the Sanctions Lists.

(14) Where an Equivalent e-document is obtained from the Customer, the Company will verify the Digital Signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder.

(15) Where an opinion is formed about suspicion of money laundering or terrorist financing, and the person carrying out CDD has reason to believe that performing the CDD process will tip-off the Customer then the CDD process should not be pursued and instead inform the Principal Officer to file STR with FIU-IND.

II. Risk Management:

Important elements of Risk Management are:

(1) Risk Assessment:

(a) Risk Assessment will be undertaken based on parameters such as Customer's identity, social/financial status, nature of business activity, and information about the Customer's business and their location, types of Transaction undertaken with the Company (cash/ cheque/monetary instruments, etc.) While considering Customer's identity, the ability to confirm identity

documents through online or other services offered by issuing authorities or Central KYC Record Registry will be considered.

(b) Risk Assessment with regard to 'Money Laundering (ML) and Terrorist Financing (TF) (hereinafter referred to as 'AML Risk) 'will have to be carried out annually to identify, assess the AML Risk and take effective measures to mitigate such risk. 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, sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time, shall have to be considered

(c) The risk assessment will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

(d) The outcome of the Risk Assessment exercise will have to be placed before the Risk Management Committee of the Company and will be made available to competent authorities and self-regulating bodies, whenever required

(e) Risk assessments should also include "Risk Based Approach (RBA)" for mitigation and management of the identified Risks and controls.

(2) **Risk Classification / Categorisation criteria**

(a) For Risk Classification / categorisation, a risk-based approach will have to be followed. Successful implementation of a risk-based approach to combat money-laundering and terrorist financing and avoiding engaging directly with Customers, if any are listed in Sanctioned List, or regions depends on a sound understanding of the threats and vulnerabilities to the Company.

(b) At the time of on-boarding, all Customers will be classified as Low/Medium or High-risk category, based on the Risk Assessment and risk perception of the Company as specified in sub section (1) above.

(c) The parameters of risk perception in terms of the nature of business activity, location of Customer, mode of payments, volume of turnover, social and financial status, etc. will be captured at the account opening stage to enable categorization of Customers into Low/ Medium/High Risk.

(d) The risk categorisation of the Customer and the specific reasons for such categorisation will be kept confidential and will not be revealed to the Customer to avoid tipping off the Customer.

(e) For the purpose of risk categorization, individuals/entities whose identities and sources of wealth can be easily identified and Transactions in whose accounts by and large conform to the known profile will be categorized as Low Risk. Illustrative examples of Low-Risk Customers are as follows:

(i) Salaried employees whose salary structures are well defined;

(ii) Government Departments and Government owned companies;

(iii) Public companies listed on recognised stock exchanges subject to disclosure requirements to ensure adequate transparency of Beneficial Owner;

(iv) Entities whose identities and sources of fund can be easily identified; and

(v) Regulators and statutory bodies, etc.

(f) Risk Categorisation of Obligors will be as per the details mentioned in **Exhibit 4.** Such Risk Categorisation of Obligors will have to be reviewed once in six months by Chief Risk Officer. The Obligors with High-Risk classification shall be subject to enhance due diligence in terms of obtaining latest KYC documents [as per Periodicity specified in Clause (6) below], verification of business activities, repayment status, status of CIBIL records etc

(g) All Non-face-to-face Customers will be subjected to enhanced monitoring until the identity of the Customer is verified in face-to-face manner or through V-CIP.

Note: *This Clause is applicable for all cases wherein, Obligor's KYC Documents are received through any digital channel such as C-KYC, DigiLocker, Equivalent e-documents, etc.*

(h) Geographic risk is important in any assessment of sanctions risk with respect to High-Risk Countries, as referred in the list enclosed as Exhibit 3. Under no circumstances financial transaction should be carried with the Customers based at/ associated from any of these High-Risk Countries

Note: The list of High Risk Countries will be updated as and when there is an updation from ORIX Corporation and same will be done with the approval of Chief Compliance Officer

(3) **<u>Customer Identification Procedure:</u>**

(a) Undertake Customer Identification in the following cases:

(i) Commencement of an account-based relationship with the Customer

(ii) When there is a doubt about the authenticity or adequacy of the Customer identification data obtained.

(iii) While carrying out Transaction (including occasional), with the Customer including Walk-in Customer, of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations.

Explanation:

(a) obtaining information on the purpose and intended nature of the business relationship, where applicable.

(b) Taking reasonable steps to understand the nature of the Customer's business, and its ownership and control;

(c) Determining whether the Customer is acting on behalf of a Beneficial Owner and identifying the Beneficial Owner and taking all steps to verify the identity of the Beneficial Owner,

Note: Identification procedure will have also be carried out in case Company is undertaking international money transfer operation with TPA. Pl refer TPA Protocol for further details

(4) **Customer Due Diligence Process:**

Customer Due Diligence need to be performed before entering into and during the relationship with the Customer to ensure that the Customer's Identity and potential money laundering, terrorist financing and sanctions risks from the relationship are responsibly evaluated and managed.

(i) **CDD for Individual Customer**:

- Please refer **Exhibit 5** for CDD process of Individuals

(ii) **CDD for Non-Individual Customer**

- Please refer **Exhibit 6** for CDD process of Non-Individuals

(iii) **CDD for PEP Customer**

No Customer will be onboarded who is identified as PEP. In exceptional cases PEP Customers may be onboarded subject to compliance of following procedure:

- In case Customer is an Individual or Non-Individual, Follow the CDD Process as described above for Individual/ Non-Individual, as the case may be; and

- Obtain prior written approval of Head of Credit & Head of Compliance or his designates.

- Please refer **Exhibit 7** for CDD process of PEP Customers.

(iv) **CDD for Non Face to Face Customer.**

- Please refer **Exhibit 8** for CDD process of NFFC accounts

(5) **On-going Due Diligence (Monitoring of Transactions)**

(a) The money laundering, terrorist financing and sanctions risks for some Customers may only become evident once the Customer has begun transacting either through an account or otherwise in the relationship with the Company. This makes appropriate and reasonable monitoring of Customer Transactions an essential component of a properly designed risk-based approach; however, it is not necessary to monitor all Transactions, accounts or Customers in exactly the same way.

(b) Undertake on-going due diligence of Customers to ensure that their Transactions are consistent with the knowledge about the Customers, Customers' business and risk profile; and the source of funds.

(c) Some form of monitoring, whether it is automated, manual, a review of exception reports or a combination of acceptable options, depending on the risks presented, will have to be done in order to detect unusual and hence possibly Suspicious Transaction. Monitoring is needed even for Customers classified as Low or Medium Risk to verify that Transactions match the initial Low/Medium Risk classification and if not, trigger a process for appropriately revising the Customer's risk classification.

(d) No financial transaction should be carried out with person who is not an Obligor of the Company unless Anti Money laundering declaration, as per the draft enclosed as **Exhibit-9** is obtained and where value of such Transaction (Single) exceeds Rs 50,000, PAN will have to be obtained from such persons.

(e) All Customers and their Transactions must be monitored and reviewed on a periodic basic (risk-based) during the business relationship to determine if the risk classification remains suitable and if the Customer documentation remains current and when there is suspicion of AML Risk or other high-risk scenarios, the identity of the Customer will be established as per Exhibit 5 or Exhibit 6, as the case may be

(f) On a periodic basis (no less frequently than quarterly or within 30 days of release of updated Sanctioned Lists by UNSC or RBI, whichever is earlier), the Chief Risk Officer or his /her designee will check the names

of the existing Obligor(s) against the Sanction List to evaluate match, if any for further process

(6) **Periodic Updation of KYC:**

(a) The risk classifications of Obligors are dynamic and may change over time. Therefore, Periodic Updation of KYC needs to be carried out at following frequency from the date of opening of the account / last KYC updation:

Sr. No.	Risk Classification	Periodicity of KYC Updation
1	High	2 Years
2	Medium	8 Years
3	Low	10 Years

(i) A review should be undertaken immediately:

- When an unusual Transaction / Suspicious Transaction is detected; or
- When there are doubts about the veracity or adequacy of previously obtained Customer identification data.

Note: Please refer Third Party Agent Protocol for risk classification of TPA

(b) Guidelines for Periodic Updation of KYC**:**

Sr. No.	**Scenario**	**Individual Customers**	**Non-Individual Customers (Legal Entities)**
1	**No Change in KYC Information**	A self-declaration from the Customer in this regard shall be obtained through Customer's email-id / mobile number registered with the Company or; through a letter confirmation. However if Customer does not provide self-declaration then the Company will send a written letter (negative confirmation	A self-declaration in this regard shall be obtained from the LE through its email id registered with the Company or; through a letter from any official authorized by the Customer in this regard, board resolution, etc. However if Customer does not provide self-declaration then the Company will send a written letter (negative confirmation letter) at last available address with the Company

		letter) at last available address with the Company	
2	**Change in KYC Information**	Fresh KYC documents as applicable for on-boarding a new Individual Customer.	Fresh KYC documents as applicable for on-boarding a new LE Customer.
3	**Change in address**	A certified copy of OVD or deemed OVD or the Equivalent e-documents thereof, confirming revised address of Customer. or *A self-declaration of the new address shall be obtained from the Customer through Customer's email-id / mobile number registered with the Company, or; through a letter. *However, in such case the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.	
4	**Change in BO**		**Latest shareholding pattern with details of updated names of BOs.**

(c) Additional Measures**:**

(i) Ensure that during Periodic Updation, the Customers are migrated to the current CDD standard.

Note: At the time of Periodic Updation, it is to be ensured that Customer's documents as specified in current KYC & AML Policy

(This Policy) are obtained, this is applicable even if there is no change in Customer information but the documents available are not as per the current CDD standards

(ii) Ensure that Beneficial Ownership (BO) information of Non Individual (Legal Entity) Customers as available with them is accurate and will update the same, if required, to keep it as up-to-date as possible.

(iii) Ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

(iv) In case the validity of the CDD documents available with the Company has expired at the time of Periodic Updation of KYC, the Company will undertake the KYC process equivalent to that applicable for on-boarding a new Customer.

(v) Customer's PAN detail is verified from the database of the issuing authority at the time of Periodic Updation of KYC.

(vi) It shall be ensured that the information / documents obtained from the Customers at the time of Periodic Updation of KYC are promptly updated in the records / database of CKYCR and an acknowledgment, mentioning the date of receipt of relevant documents and date of updation of KYC details, is provided to the Customer.

(vii) Alternatively, a Customer on his free-will can also visit any of the Company's branch for the purpose of Periodic Updation of KYC.

(viii) In case, an Obligor is an Individual, his/her recent photograph will also be obtained along with Periodic Updation of his/her KYC Records.

F. <u>OTHER ELEMENTS OF THE POLICY</u>:

I. Record Management

(1) <u>Maintenance of records of Transactions</u>:

The Company will maintain proper record of the Transactions as required under Section 12 of the Act, read with Rule 3 of the Rules as mentioned below:

(a) All cash Transactions of the value of more than Rs. 10,00,000 (Rupees Ten Lakhs);

(b) All series of cash Transactions integrally connected to each other which have been valued below Rs. 10,00,000 (Rupees Ten Lakhs) where such series of Transactions have taken place within a month;

(c) All cash Transactions where forged or counterfeit currency notes or bank notes have been used and / or attempted to be used as genuine;

(d) Any such Transactions records pertaining to identification of the Customer and its/his/her address; and

(e) All Suspicious Transactions whether or not made in cash and in manner as mentioned in the Rule.

(2) **Records to contain the specified information**

The Records referred to Sub Para (1) above Rule 3 of PMLA Rules to contain the following information:

(a) The nature of the Transactions;

(b) The amount of the Transaction and the currency in which it was denominated;

(c) The date on which the Transaction was conducted; and

(d) The parties to the Transaction.

(3) **Maintenance and preservation of records**:

Section 12 of the Act requires the Company to maintain records as under:

(a) Records of all Transactions as referred as Sub Para (1) above to be maintained for a period of five (5) years from the date of Transactions between Customers and the Company.

(b) Records of the identity and address of all Customers including documents obtained during Periodic Updation is required to be maintained for a period of five years from the date on which business relationship is ended between the Customers and the Company.

(c) The Company will take appropriate steps to evolve a system for proper maintenance and preservation information (Identification and address documents/ Transactions/Communication etc.) of all Customers, in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

(d) In addition to the documents specified in sub clause(b) above to be preserved, account files, business correspondence and results of any analysis undertaken will also be preserved for a period of 5 years from the date on which business relationship is ended

(e) The Company will ensure that in case of Customers who are non-profit organisations, the details of such Customers are registered on the DARPAN Portal of NITI Aayog or;

(f) If the same are not registered, the Company will register the details on the DARPAN Portal and shall also maintain such registration records for a period of five years after the business relationship with the Customer has ended or the account has been closed, whichever is later.

II. Secrecy Obligations and Sharing of Information:

(1) The Company will maintain secrecy regarding the Customer information, which arises out of the contractual relationship between the Company and Customers.

(2) Information collected from Customers for opening of account shall be treated as confidential and details thereof will not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the Customer;

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

(4) The exceptions to the said rule will be as under:

(a) Where disclosure is under compulsion of law / directives of the RBI;
(b) Where there is a duty to the public to disclose;
(c) the interest of the Company requires disclosure; and
(d) Where the disclosure is made with the express or implied consent of the Customer.

(5) The Company will maintain confidentiality of information as provided in Section 45NB of RBI Act 1934 or to FIU-IND.

III. Reporting:

(1) The Principal Officer will report Suspicious Transactions and/or Red-flags to **Financial Intelligence Unit – India (FIU-IND)** In accordance with the requirements under Act.

(2) The Principal Officer of the Company will furnish the following reports, as and when required, to the Director, FIU-IND:

(i) Cash Transaction Report (CTR) – If any such Transactions detected, CTR for each month by 15th of the succeeding month;

(ii) Counterfeit Currency Report (CCR) – All such cash Transactions where forged or counterfeit Indian currency notes have been used as genuine as CCR for each month by 15th of the succeeding month;

(iii) The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any Transaction, whether cash or non-cash, or a series of Transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, no restriction shall be put on operations in the accounts where an STR has been filed.

(iv) Details of accounts resembling any of the individuals/entities in the Sanction Lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA).

(3) The Principal Officer while furnishing relevant information to the FIU-INDIA, shall also take note and adhere to the guidelines issued by FIU-INDIA on detection of transactions referred in various clauses of sub-rule (1) of rule 3 and directions on the form of furnishing information and specification about the procedure and the manner of furnishing CTR / STR. Timeliness as specified by FIU for various returns needs to be adhered.[6]

(4) No restrictions shall be put on operations in the accounts where an STR has been filed and it shall keep the fact of furnishing of STR strictly confidential, without tipping off to the Customer at any level.

(5) In case, when a suspicion of money laundering or terrorist financing has been formed, and it is reasonably believed that performing the CDD process will tip-off the Customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

(6) Robust software, throwing alerts when the Transactions are inconsistent with risk categorization and updated profile of the Customers shall be put in to use as a part of effective identification and reporting of suspicious Transactions.

(7) Any employee who become aware of questionable conduct or potentially "Suspicious Transaction" or any "Red Flags" that may indicate potential money laundering or evasion of economic sanctions activities, regardless of the amount of the Transaction, to immediately report any such Suspicious Transaction or "Red Flags" to the Principal Officer and the Compliance Officer.

---

[6] 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 CTR /STR, which FIU-IND has placed on its website, shall be used by the Company. The Principal Officers shall put in place suitable arrangement to cull out the Transaction details from branches and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in

(8) The Principal Officer must inquire more fully into circumstances and take whatever steps which are necessary and appropriate, including taking any other corrective or remedial steps, in all cases complying with secrecy obligations regarding reported Transactions; assisting employees with reporting responsibilities they may have; independently reporting the Suspicious Transaction or activity to the appropriate government agency or regulatory authority.

IV. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(1) Ensure that identity of any Customer does not match with any person or entity, whose name appears in the United Nations Sanctions list, as mentioned below, with suitable systems in place:

(a) **The "ISIL (Da'esh) &Al-Qaida Sanctions List"**

This includes names of individuals and entities associated with the Al- Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

(b) **The "Taliban Sanctions List"**

This includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.html

(c) **UNSCR 1718 Sanctions List**

This includes names of Individuals and Entities, as available at https://www.mea.gov.in/Implementationof-UNSC-Sanctions-DPRK.htm. This list shall be verified every day.

V. The Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

(1) Ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India

(2) Not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list for WMD Act, 2005 available at FIU-India (fiuindia.gov.in).

(3) The Company to run a check, on the given parameters, at the time of establishing a relation with a Customer and on a periodic basis (semi-annually) to verify whether individuals and entities fall under the designated list as mentioned in Clause IV (1) above.

(4) In case of match in the above cases, the Company will immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication will be sent to State Nodal Officer, where the account / transaction is held and to the RBI. The Company will file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

(5) Undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

In case there are reasons to believe beyond doubt that funds or assets held by a Customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the Company will prevent such Customer from conducting Transactions, under intimation to the Central Nodal Officer by email, .and by post, without delay

VI. Appointment of Designated Officials as required under the Act:

(1) **Principal Officer**:

The Principal Officer will be responsible for ensuring compliance, monitoring Transactions, and sharing and reporting information as required under the law/regulations as per the roles and responsibilities approved by the Management.

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

(2) **Designated Director:**

The Board of Directors of the Company hereby designates the Managing Director/Whole Time Director, who oversees the operations of the Company, as the Designated Director of the Company to ensure overall compliance with the obligations imposed under Act and the Rules. The Company will communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND.

VII. Roles and Responsibilities of Designated Officials and Senior Management:

(1) **Designated Officials**:

(a) **Designated Director**:

To ensure overall compliance with the obligations imposed under Act and the Rules

(b) **Principal Officer**:

(I) Reporting of Suspicious Transaction and Red flags as reported by Responsible Person mentioned in Exhibit 11 to FIU-IND & to Chief Compliance officer

(II) Reporting of Red Flags to Chief Compliance Officer

(III) Submission of CTR, CCR and STR to FIU-IND within time stipulated in this Policy.

Note: The STR shall include details of accounts resembling any of the individuals/entities featured in the Sanctioned List which shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA

(IV) Review prevailing regulatory guidelines on Money Laundering and recommend to Chief Compliance Officer suggested changes in the Policy

(V) Handling queries from the RBI or any other regulator or statutory body with regard to this Policy and AML Policies and procedure adopted in consultation with Chief Compliance Officer

(2) <u>Senior Management</u>:

(a) **Chief Compliance Officer**:

(I) Review the Policy on a periodic basis (at least once in a year or as and when regulatory changes announced) with the Principal Officer and Chief Risk Officer and make suitable changes in the Policy

(II) Training of relevant staff on KYC & AML aspects specified in this Policy

(III) Reporting of Suspicious Transaction Global Compliance Team, ORIX Corporation & Suspicious Transaction and Red Flags Audit Committee.

(IV) Support other Senior Management team members in designing framework / process for implementation of this Policy

(V) The CCO will identify and undertake the AML Risk Assessments that may arise in relation to the development of new products and new business practices.

(b) **Chief Risk Officer (Head of Credit)**

(I) Risk categorization for Customers before on boarding

(II) Periodic Risk Assessment & Maintenance of Records.

(III) Ensuring KYC documents compliances as per the Policy for all the Obligors of the Company

(IV) Suspicious Transaction and Red flags monitoring as specified in Exhibit 11

(V) Ascertaining the details of Beneficial Owners in applicable cases.

(VI) Verifying Obligors / Beneficial Owner against Sanctioned List as well as at the time of On Boarding & as per periodicity defined in the Policy and report to the Chief Compliance Officer and Principal Officer, if any match is found

(VII) Maintain the Details of PEP Customers via system flagging

(VIII) Submitting Obligors details to C-KYC Portal within 10 days of on-boarding and follow the process regarding updation of CKY Records Registry as specified in Exhibit 10.

(IX) Identifying geographic locations that may pose a higher risk and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating Transactions involving certain geographic locations

(X) Informing Chief Compliance Officer whenever any positive match for existing / prospective Obligors with Sanction List.

(XI) Carry out AML Risk Assessment exercise annually to identify and assess AML Risk and take effective measures to mitigate such risk and put up for review of Audit Committee.

(XII) carry out periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures.

(XIII) Meticulous compliance with the Order issued by the Government under Section 51A of UAPA with regard to freezing of Assets of individual or entities listed in Sanctioned List shall have to be followed.

(c) **Head of Operations**:

(I) Ensuring KYC documents compliances as per the Policy for all the Loan Against Property Business's Obligors & Third Party Agents of the Company

(II) Ensure AML Declaration is obtained wherever payments are received from any person other than Obligor

(III) Coordinating with IT & Compliance so as to decide the framework & develop the system capabilities to monitor Suspicious Transaction and Red-flags

(IV) Suspicious Transaction and Red flags monitoring as specified in Exhibit 11

(V) Reporting Suspicious Transaction to Principal Officer for onward reporting to FIU India

(VI) Reporting Red Flags as referred in Exhibit 11 to Chief Compliance Officer

(VII) Maintenance of all record as per record management policy (Hard Copy of records)

(VIII) Ensure that no new Customer is on boarded without following CDD Process

(IX) Information collected from Customers for opening of account shall be treated as confidential (Hard Copy of records)

(X) Trail of movement of physical files (From branch to storage vendor & vice versa) should be maintained.

(XI) Ensure that Payment to 'High-Risk Jurisdictions' are made as per the terms of "Payments Rules" of the Company

(XII) Ensure that in case of NFFC Customers, current address proof is available in the Company's records and operations in the account are allowed only after positive confirmation of current address by any means such as address verification letter, contact point verification, deliverables, etc.

(XIII) Ensure that any account is opened only after Due Diligence Process as mentioned in Exhibit no 5,6,7 & 8 are followed.

(d) **Head of Information Technology**:

(I) Unique UCIC mapping for each Obligors for all products of the Company

(II) System upgradation for Suspicious Transaction and Red-flags Monitoring

(III) Provisions for Reports of Risk categorization & ongoing Due Diligence for all Customers of the Company

(IV) Information collected from Customers for opening of account shall be treated as confidential (Soft Copy of records)

(V) Audit trail for all the application used for on boarding/credit assessment of the Customers

(e) **Head of All Business & Functions**

(I) Ensure KYC & OVD documents are collected from all the Customers, as per the terms of this Policy & TPA Protocol, at the time on-boarding as well as at the time of periodic Risk Assessments

(II) Any Red Flag or Suspicious Transactions identified for any of Customer, as referred in Exhibit 11, shall be promptly referred to Chief Compliance Officer for further analysis.

(III) Transaction details of sale of third party products (such as insurance) shall be maintained as per the terms of this Policy.

(f) **Head of Treasury**

Ensure that Payment to 'High-Risk Jurisdictions' are made as per the terms of "Payments Rules" of the Company

(g) **Head of Internal Audit**:

(I) Independent evaluation of the Compliance of this Policy

(II) Reporting non-compliance to the Audit Committee

VIII. Customer Education, Training and Recruitment:

(1) Customer Education:

Implementation of KYC procedures requires Company to demand certain information from the Customer which may be of personal nature or which has hitherto never been called for. This sometimes leads to a lot of questioning by the

Customer as to the motive and purpose of collecting such information. The Relationship Managers of the Company will be trained to explain to the Customer, the regulatory requirements and benefits this Policy and seek co-operation of the Customer.

(2) Training: The Company will have ongoing training programme in terms of the following:

(a) Circulating information, from time to time, to the Senior Management Team wherein they are made aware about changes in this Policy

(b) All Circulars issued by the regulatory bodies are circulated to Senior Management Team

(c) Compliance Department will prepare a training module and provide periodic targeted trainings for Sales, Operations, Credit and Principal officer for areas relevant to them as per the terms of this Policy.

(3) Recruitment:

KYC norms / AML standards / CFT measures are prescribed in this Policy to ensure that criminals are not allowed to misuse Company's infrastructure. It should therefore be necessary that the Company, as an integral part of their recruitment, put in place adequate screening mechanism / hiring process of personnel.

IX. Updation:

Given the fact that the risks the Company faces are constantly changing, and that money laundering risk management methodologies, regulations and tools are evolving, it is imperative that this Policy document be reviewed on annual basis or earlier when there are significant changes in the applicable AML regulations.

Exhibit 1

List of Officially Valid Document's (OVD)

Sr. No.	Category	Certified Copy of Documents / Equivalent e-documents
1A	Individual -Resident; Proprietor; Persons such as partner, director, employee, manager, trustee, etc. holding an attorney to transact on the behalf of legal	(a) PAN or Form 60 at the time of acceptance of new Customer. However, Customer has to submit copy of PAN card within sixty days from the date of application as submission of PAN is mandatory; and (b) One copy of an Officially Valid Document (OVD) List of OVDs: - (i) Passport (ii) Driving Licence (iii) Voter's Identity Card issued by Election Commission of India (iv) Job card issued by NREGA duly signed by an officer of the State Government (v) The letter issued by the National Population Register containing details of name, address (vi) Offline Verification of Aadhaar Card or through OTP based verification or Masked Aadhaar Card Downloaded from UIDAI website (vii) Manually masked Aadhaar Card should be accepted only after OSV verification from the Company Employee and (c) One recent Photograph (of the Borrower and Co-Lessee)
1B	Individual-Non-Resident Indian (NRI) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}	Certified Copy of KYC documents of country of residence, certified by any one of the following, may be obtained: (a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India, (b) branches of overseas banks with whom Indian banks have relationships, (c) Notary Public abroad, (d) Court Magistrate, (e) Judge,

		(f) Indian Embassy/Consulate General in the country where NRI Customer resides.
1C	Individual - Foreign National - (where he / she is acting for and on behalf of Non Individual Customer or Legal Entity)	Certified Copy of KYC documents of country of residence, certified by notary officer or Non-Individual Customer for whom the Foreign National is acting alongwith the authority letter from such Non-Individual Customer authorising him / her to act on behalf of such Non-Individual Customer
2	Sole Proprietorship Firm	In addition to the documents as stated in category (1) above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained: - (a) Registration certificate including Udhyam Registration Certificate (URC) issued by Government. (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act (c) Sales and income tax returns (d) Certificate/registration document issued by CST/VAT/ GST /Professional Tax authorities (e) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute (f) 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 (g) Utility bills such as electricity, water, land line telephone bills, etc. **Note:** In cases where it is not possible for Customers to furnish two such documents, Chief Compliance Officer or his designate may, at its discretion, accept only one of those documents as proof of business / activity provided: (i) They are satisfied that it is not possible for Customer to provide two such documents; (ii) Positive contact point verification is conducted 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.
3	Legal Entities	(a) Certificate of incorporation (b) Memorandum and Articles of Association (only first 2/3 pages where Main object(s) is/are specified (c) Permanent Account Number of the company (d) Certificate/registration document issued by CST/VAT/ GST /Professional Tax authorities (e) IEC (Importer Exporter Code) issued by the office of DGFT (f) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf (g) Documents, as specified in Sr. no 1, relating to Beneficial Owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the Company's behalf (h) The names of the relevant persons holding senior management position (i) The registered office and the principal place of its business, if it is different
4	Partnership firm / LLP	(a) Registration certificate (b) Partnership deed (c) Permanent Account Number of the partnership firm / LLP (d) Certificate/registration document issued by CST/VAT/ GST /Professional Tax authorities (e) Documents, as specified in Sr. no 1 relating to Beneficial Owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf (f) The names of all the partners (g) Address of the registered office and the principal place of its business, if it is different
5	Trust	(a) Registration certificate (b) Trust deed (c) Permanent Account Number or Form No. 60 of the trust (d) Documents, as specified in Sr. no 1 relating to Beneficial Owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf (e) The names of the beneficiaries, trustees, settlor protector, if any and authors of the trust

		(f) List of Trustees and documents, as specified in Sr. no 1, for those discharging the roles as trustee and authorised to transact on behalf of the trust (g) The address of the registered office of the Trust.
6	Unincorporated association or a body of individuals	(a) Resolution of the managing body of such association or body of individuals (b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals (c) Power of attorney granted to transact on its behalf (d) Relating to Beneficial Owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf & Documents, as specified in Sr no 1 (e) Such Information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals **Explanation:** Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and Term 'body of individuals' includes societies.
7	Juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats	(a) Document showing name of the person authorised to act on behalf of the entity; (b) Documents, as specified in Sr. no 1, of the person holding an attorney to transact on its behalf; and (c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Exhibit 2 – Digital KYC Process

(1) The Company will develop an application for digital KYC process which shall be made available at Customer touch points for undertaking KYC of Customers and the KYC process shall be undertaken only through this authenticated Application of the Company.

(2) The access of the Application shall be controlled by the Company, and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

(3) The Customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

(4) The Company must ensure that the Live photograph of the Customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company will put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the Customer.

(5) The Application of the Company will have the feature that only live photograph of the Customer is captured and no printed or video-graphed photograph of the Customers is captured. The background behind the Customers while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the Customer.

(6) Similarly, the live photograph of the original officially valid document or proof of possession of Aadhaar where Offline Verification cannot be carried out (placed horizontally), shall be captured vertically from above and watermarking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

(7) The live photograph of the Customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

(8) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the Customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

(9) Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to Customer’s own mobile number. Upon successful validation of the OTP, it will be

treated as Customer signature on CAF. However, if the Customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the Company will not be used for Customer's signature. The Company must check that the mobile number used in Customer's signature shall not be the mobile number of the authorized officer.

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

(11) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the Transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding Transaction-id/reference-id number to Customer for future reference.

(12) The authorized officer of the Company will check and verify that:

(a) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(b) live photograph of the Customer matches with the photo available in the document; and

(c) all of the necessary details in CAF including mandatory field are filled properly.

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

Exhibit 3

List of High-Risk Jurisdictions

Exhibit III.docx

Exhibit 4

Risk Categorisation of Customers shall be as under:

(i) Risk Categorisation for Accounts in the Name of Individuals:

Type	Recommended Risk Categorization	Risk Perception
Salaried Customer associated with any of the High-Risk Industry [As referred in point no (iii)]	High Risk	Individuals associated with High Risk industries are more prone to money laundering risk and the Company needs to be extra vigilant on those set of Customers.
Senior citizens, Housewife	High Risk (if they are main Borrower)	Probability of such accounts being operated by third parties are high.
Non-Resident Individual	High Risk	Income in Foreign Currency & various statutory regulations applicable to them
Politically Exposed Person	High Risk	It is global practise to treat such cases as HIGH Risk.
Salaried- Working with Pvt Ltd Companies or Partnership firms or LLP	Medium or Low Risk	Medium: Salaried applicants with only variable income, receiving salary in cheque. Low: If salary is structured and uniform.
Salaried- Working with Public Ltd Companies	Low Risk	Source on income is fixed and pattern of entries in the account can be correlated with known sources of income/expenditure.
Self Employed	Low Risk	All Self-employed Customer other than the one associated with High Risk Industries should be tagged as Low Risk

(ii) Risk Categorisation for Accounts in the Name of Non-Individuals

Type	Recommended Risk Categorization	Risk Perception
Trusts – Public Charitable Trust/ NGO's and any other organization accepting donations	High Risk	The pattern of entries in the account may not be correlated with known sources of Income/expenditure.
Trusts – Private Trust	High Risk	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known sources of income/expenditure.
Trusts – Registered	Low Risk	To be considered as Low Risk due to registration.
Societies / Clubs /Associations	High Risk	These are not highly regulated entities and the pattern of entries in the account may not be correlated with known sources of income/expenditure.
NFFC Customers	High Risk	As per recent RBI Guidelines
Multi-Level Marketing Companies (MLM)	High Risk	MLM Companies are more prone to money laundering risk due their nature of business
Pvt Ltd Companies	High / Medium / Low Risk	Depending on the clarity of the shareholding structure and the nature of operations, such companies would be classified.
Hindu Undivided Family (HUF)	Medium Risk	These are unregistered bodies and the pattern of entries in the account may not be correlated with known sources of Income/expenditure.
Public Ltd. Companies	Low Risk	Listed entities with proper disclosures in public domain.

Local Authorities or Public Bodies	Low Risk	They are constituted under Special Acts. Operations are governed by such Acts/Rules.
Public Sector Undertakings, Government Departments or Statutory Corporations	Low Risk	These types of entities are governed by specific Acts, Notifications, etc. framed by the Government of India or the State Govt. and are controlled and run by the Govt.
Mutual Funds/Scheduled Commercial Banks/Insurance companies/Financial Institutions	Low Risk	These entities are strictly regulated by their respective regulators.

(iii) <u>Risk Categorisation on the basis of Industry</u>

The Risk categorization is dependent on industries which are inherently High Risk or may exhibit high cash intensity, as below**:**

No	Industry
(a)	Arms Dealers
(b)	Money Changer Exchange houses
(c)	Gems / Jewelry / Precious metals / Bullion dealers (including sub-dealers) / Real Estate Agents
(d)	Construction / Offshore Corporation
(e)	Bar / casino / night club / Import/Export agents (traders; goods not used for own Manufacturing/retailing) / Share & Stockbrokers
(f)	Art/antique dealers
(g)	Auto dealers (used/reconditioned vehicles/motorcycles)
(h)	Business activity relating to Real estate, convenience stores, vending machine operators, and parking garages
(i)	Virtual Currencies
(j)	Marijuana, liquor stores, Liquor distributorship
(k)	Scrap metal dealers
(l)	Commodities middlemen
(m)	Co-operative Banks
(n)	Multi Level Marketing (MLM) Firms
(o)	All other industries basis the nature of business (as and when required to be included)

Exhibit 5

CDD Process in case where an Obligor (Individual)

(1) Obtain OVD of the Obligor either for permanent or current address proof. Please refer Exhibit 1 for further details.

(2) Obligor's personal email id and Mobile Number (should preferably be linked to his / her Aadhaar) should preferably be obtained.

(3) In case Obligor submits a KYC Identifier (C-KYC number) or his explicit consent to download his KYC records from the CKYCR, then retrieve the KYC records online from the CKYCR. In such case, obtain his current address details (if current address is different than permanent address) as mentioned above obtain his/her PAN copy or form No. 60., if same is not available in CKYC records.

Note: In such cases:

(a) No other OVD shall be required;

(b) Obligor *shall not require to submit the same KYC records or information or any other additional identification documents or details, unless –*

- *there is a change in the information of such Obligor as existing in the records of Central KYC Records Registry.*
- *the current address of such Obligor is required to be verified. Further, if Customer wants to provide a current address, different from the address as per identity information available in CKYCR and self-declaration about the provision of current address should be sought.*

(4) Process laid down in Point (5) below need not be followed if Obligor submits any of following Documents:

(i) Aadhaar card with Offline Verification; or

Note: If Customer submits a copy of possession of Aadhaar number containing Aadhaar number, ensure that such Customer redacts or blacks out the first 8 digits of his / her Aadhaar Number.

(ii) Masked Aadhaar card downloaded from UIDAI Portal

(iii) Documents shared through Digi Locker or Equivalent E -documents issued by issuing authority.

Note: *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 Obligor.*

(5) Physical verification of OVD: if documents as mentioned in Point (1) above is not provided by Obligor then the employee is required to verify the certified true copy of OVD with the original and shall have to affix their name, signature, employee ID as well as date of verification on certified true copy of OVD and also state on such certified true copy '<u>Original seen and verified</u>';

~~(6)~~ Obtain most recent passport size colour photograph of Obligor

(7) In case of Walk-in Obligor (person other than account holder), where the amount involved is equal to or exceeds Rs 50,000 (in cash), whether conducted as a single Transaction or several Transactions that appear to be connected, the CDD process as listed above need not be followed, however copy of PAN needs to be obtained

(8) Such other documents including in respect of the nature of business and financial status of the Customers.

(9) If the Customer has provided Equivalent e-document, then verify the Digital Signature as per the I.T. Act and / or Rules issued thereunder.

Exhibit 6

CDD Process for Obligor who is Non-Individual

(Whether Sole Proprietor / Private or Public Limited Company / Partnership Firm/ LLP / Society / Trust)

(a) Identify such Obligor by obtaining KYC documents as more particularly specified in the **Exhibit 1** of this Policy.

Note: For on-boarding Sole proprietor as a Customer, CDD of Individual (Proprietor) shall have to be carried out.

(b) Ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out Transactions as specified in Customer Identification Procedure under Clause II (3).

(c) Identify the representative and management of such Obligor and verify the identity of those individuals in order to be able to perform a screening on the management of such Obligor and ensure that the persons purporting to act on behalf of such Obligor are authorized to do so.

Note*:*

(a) *Obtain OVD of authorized representative of such Obligor at the time of onboarding & carry out the process as stated in point number (1) above.*

(b) *Obtain document such as Board Resolution or Power of Attorney authorising person to transact on and behalf of Obligor (in case of Finance Lease and Loan Transaction).*

(c) *If above document is not available, then obtain letter or email confirmation from the Company Secretary or Director of the Company (other than authorised person) to confirm the authority of authorised person*

(d) Beneficial Owner (BO) and taking reasonable measures to verify the identity of the BO.

Note*:*

(a) *Where BO cannot be identified by reference to shareholding, voting rights or ownership, the Obligor's managing director or chief executive will be designated as the beneficial owner.*

(b) *BO details shall have to be obtained only in case the Obligor is the PVT ltd. Company or a Public LTD Company which is not listed on recognized stock exchange of India or A Trust or Society or Partnership Firm.*

(c) *It is clarified that the BO details shall not be required if the PVT Company or Unlisted Public company is the subsidiaries listed on recognized stock exchange of India*

Exhibit 7

CDD Process for Politically Exposed Persons (PEPs)

The Company will consider establishing a relationship with PEPs provided that:

(a) Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

(b) The identity of the person shall have been verified before accepting the PEP as a Customer;

(c) The decision to open an account for a PEP is taken at a senior level in accordance with this Policy;

(d) All such accounts are Categorized as 'HIGH Risk' & subjected to enhanced monitoring on an on-going basis;

(e) In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, CRO & CCO or his designates approval is obtained to continue the business relationship;

(f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

(g) These instructions shall also be applicable to accounts where a PEP is the beneficial owner or family members or close associates of PEPs

Exhibit 8

CDD Process for NFFC

(a) Apart from obtaining the current address proof, verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

(b) NFFC Customers shall be categorized as high-risk Customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the Customer is verified in face-to-face manner

Transactions in NFFC accounts shall be permitted only from the mobile number used for account opening.

(c) Alternate mobile numbers of any Customers shall not be linked post CDD with NFFC accounts for Transaction updates, unless the procedures of updating mobile numbers as per approved Business / Operations SOPs are diligently followed.

Exhibit 9

To,

The Manager,

ORIX Leasing & Financial Services India Ltd (OLFS)

Sir,

This is to confirm that I have made payment of Rs _____ to OLFS, as per the details mentioned below on behalf of _____ (Borrower) towards the Loan Account Number _____.

I have made this payment voluntarily to help _____ (Borrower) who is my Relative/Friend/ Business associates etc [please select as appropriate] and I hereby undertake that I shall not lay any claim in future from OLFS In lieu of this payment.

I hereby confirm that amount paid by me is my clean money earned through legitimate source, I also confirm that I am no way involved in any kind of activity such as Money Laundering, Tax evasion etc. which is prohibited by law.

I authorize OLFS to share my payment details with Statutory Authorities/Law enforcement agencies etc. in case if it is required as per applicable Laws of India

Payment details are as mentioned:

Mode of Payment: - Cheque/Demand Draft/ Online Payment /Cash

Cheque/ Demand Draft no: -

UTR No: -

Payee bank: -

Bank account No: -

Name of Bank Branch: -

Date of Transaction: -

Thanks

Name: -

Date: -

Signature: -

Exhibit 10

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

(1) Capture Customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the Customer, with adherence to Operational Guidelines for uploading the KYC data as released by CERSAI.

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

(3) Upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR. The KYC records have to be uploaded as per the LE Template released by CERSAI. For accounts opened prior to April 1, 2021, CKYC records shall be updated at the time of Periodic Updation of KYC or when the updated KYC information is obtained/received from the Customer (whichever is earlier), as per the terms of this Policy.

(4) Once KYC Identifier is generated by CKYCR, ensure that the same is communicated to the individual / LE on their registered contact details.

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

   (i) There is a change in the information of the Customer as existing in the records of CKYCR;

   (ii) The current address of the Customer is required to be verified;

   (iii) The Company considers it necessary in order to verify the identity or address of the Customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

   (iv) The validity period of documents downloaded from CKYCR has lapsed.

Exhibit 11

Following are the indicative list of Suspicious Transactions and Red Flags which are bifurcated into Regulatory and Non-Regulatory, respectively. [Regulatory means Suspicious Transactions which are required to be reported to Principal Officer for onwards reporting to FIU-IND under PMLA and RBI Master Direction and Non-Regulatory are those which are required to be reported to Chief Compliance Officer or his designate]

Sr, No	**Suspicious Transactions and/or Red-Flags**	Department Responsible for Reporting
(1)	**Regulatory**	
	(a) Obligor's documents identified as forged, after onboarding	Credit and/or Operations
	(b) Monthly instalments sought to be paid in cash which breaches the threshold value as specified in PMLA	Operations
	(c) all cash transactions of the value of more than rupees ten lakhs (100000) or its equivalent in foreign currency	Operations
	(d) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.	Operations
	(e) Obligor seeking to pre-pay loan (part/full) in cash where the amount involved is more than Rs 2,00,000 in single transaction	Operations
	(f) Monthly instalments / part payment received from a third-party bank account on regular basis (3 months in a year, during the Lease/ Loan Tenure), unless the **AML declaration as referred in Exhibit 9 above** is obtained.	Operations
	(g) The existence of accounts of Obligors or Beneficial Owner in High Risk Countries	Credit
(2)	**Non-Regulatory (Red flags)**	
	(a) Prospective Obligor attempts to obtain any financial facility basis the forged document	All Business & Functional Units and/or Credit

	(b) Negative media, news with respect to the Customer	All Business & Functional Units and/or Credit
	(c) Welcome letter undelivered after 2 attempts.	Operations
	(d) Any known case when Customer is involved in fraud / dispute over any financial transaction with any other Banks or financial institutions	All Business & Functional Units and/or Credit
	(e) Any Obligor is identified as PEP during the tenure of active relationship	All Business & Functional Units and/or Credit
	(f) Any other Transactions deemed as a suspicious in nature	Operations
	(g) Non-Individual entities which demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increased in the activity	Credit
	(h) Non-Individual entity which is registered under a name that indicates that the company performs activities or services that it does not provide without good reason	Credit

Modification History

Date of Revision	Version	Description	Authors	Approved by
13-06-2005	1	Initial draft in OAIS	Mr. Abhijit Chatterjee / Mr. Jay Gandhi	Board of Directors
27-07-2010	2	Updated and adopted in OAFS, being an NBFC Company	Mr. Jay Gandhi	Board of Directors
27-08-2012	3	Updated as per the Master Circular of RBI dated July 2, 2012	Mr. Parthasarathy Ray, Ms. Shuchi Singhvi and Mr. Mahesh Wad	Board of Directors
31-03-2017	4	Updated as per the RBI KYC Master Directions, 2016	Secretarial Department	Board of Directors
13-11-2018	5	Constitution of Senior Management of the Company for the purpose of KYC Compliance as per RBI KYC Master Directions, 2016	Secretarial Department	Board of Directors
29-07-2020	6	Updated as per the RBI KYC Master Directions, 2016, as amended until April 2020 and the ORIX Group Anti-Money Laundering Policy	Compliance	Board of Directors
08-04-2022	7	Approved by GGCO on 07-04-2022	Compliance	Board of Directors
11-10-2023	8	Sent to GGCO for review	Compliance	Board of Directors
21-12-2023	9	Approved by GGCO on 20-12-2023	Corporate Secretary	Board of Directors