KNOW YOUR CUSTOMER ("KYC") & ANTI MONEY LAUNDERING ("AML") POLICY OF MIZUHO CAPSAVE FINANCE PRIVATE LIMITED (FORMERLY KNOWN AS CAPSAVE FINANCE PRIVATE LIMITED)

Sr. No.	TABLE OF CONTENTS

25.	ANNEXURE-C

1. INTRODUCTION

The present KYC / AML Policy is updated incorporating guidelines issued by Statutory/Regulatory Authorities.

In terms of the provisions of PML Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, the Company being Regulated Entities (REs) are required to follow certain customer identification procedures and conduct customer due diligence while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions and take steps to ensure implementing the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s).

2. OBJECTIVE

The objective of guidelines for KYC is to standardize KYC documentation across the Company. This policy will reduce ground level ambiguity and ensure faster KYC document collection.

3. DEFINITION

''Designated Director'' means Managing Director and/or any whole time Director, duly authorised by the Board of Directors to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act, 2002 and the Rules.

''Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location of the customer from where such live photo is being taken.

''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.

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

"Customer" For the purpose of KYC norms, A customer is defined as a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

"**Officially Valid Document" (OVD)** means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election

Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

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

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

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

"Principal Officer" Principal Officer of the Company shall be responsible for furnishing information as per rule 8 of the Rules.

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

''**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.

"Beneficial Owner (BO)"

a. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
    1. Controlling ownership interest means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
    2. Control shall include the right to appoint a majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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

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

d. The 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. 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.

"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 of1961).

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

"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to reasonable grounds of suspicion that it may involve financing of the activities relating to terrorism.

4. 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.

b. 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, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

c. 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 the 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.

d. The outcome of the exercise shall be put up with 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.

5. COMPLIANCE OF KYC POLICY

The Head of Operations shall be responsible for obtaining and maintaining all KYC records from the borrowers and ensure the overview of the KYC Compliance.

Internal Auditor/Internal Audit System shall review KYC compliance as per the Policy.

a. The Audit Committee shall report in the form of a note on a quarterly basis about the status of KYC compliance in accordance with this policy.

b. The concurrent/internal auditors need to provide a quarterly update to the Audit committee on KYC compliance and the procedures to be followed.

c. The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

6. KEY ELEMENTS

The Company 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

a) Customer Acceptance Policy (CAP)

The Company shall ensure the following:

(i) No account is opened in anonymous or fictitious/ benami name(s);

(ii) 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.

(iii) No transaction or account-based relationship is undertaken without following the CDD procedure.

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

(v) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

(vi) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise if the available KYC with us is not older than 6 months.

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

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

(ix) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

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

(xi) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000). Please note that pdf sign on the document is not considered as digital signature on the document.

(xii) As advised by RBI, the company shall not allow opening and/or holding of an account on behalf of client/s by professional intermediaries, like lawyers and Chartered accountant, etc who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further any professional intermediary who is under any obligation that inhibits the company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client

(xiii) Prohibitions:

- Countries, government, entities and individuals that are subject to economic sanctions.
- List of terrorist Individuals/Organizations- Under UN Security Council resolution pursuant to resolutions 1267(1999) ,1989(2011), 2253 (2015), 2368 (2017) and similar resolutions.

(xiv) Where such information requirement has not been specified in this policy that shall be obtained with the explicit consent of the customer.

(xv) Where GST number is available, the same shall be verified through the search/ verification facility provided by the issuing authority.

Where company is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR.

b) Customer Identification Procedure (CIP)

Set out below is the Company's adopted Customer Identification Procedure that shall be

carried out at different stages, i.e.

- At time of establishing of an account-based relationship with the customer
- Carrying out a financial transaction (for non-account customers)
- When the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

The Company will obtain the information stated below necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

Being satisfied means that the Company must be able to satisfy the competent authorities 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.

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

Changes due to introduction of Video based Customer Identification Process (V-CIP)

The Company may undertake V-CIP to carry out:

i) Customer Due Diligence (CDD) in case of new customer

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

iii) Updation/Periodic updation of KYC for eligible customers based on the risk classification.

Following are the minimum standards to be followed before undertaking V CIP:

V- CIP Infrastructure

- Ensure the compliance of cyber security.
- The technology infrastructure should be housed in the own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain.

- Any technology-related outsourcing for the process should be compliant with relevant RBI guidelines.

- Ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards.

- Customer consent should be recorded in an auditable and alteration-proof manner.

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

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

- Application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company.

- Technology infrastructure including application software as well as workflows shall be regularly upgraded.

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

- V-CIP infrastructure shall undergo necessary tests, such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities.

V – CIP Procedure

- A clear workflow and standard operating procedure for V-CIP shall be formulated and should be adhered to it.

- V-CIP process shall be operated only by officials of the Company specially trained for this purpose.

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

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

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

- The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information as prescribed.

- In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 working days from the date of carrying out V-CIP.

- Ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication /equivalent e-document.

- Economic and financial profile/information submitted by the customer to be confirmed.

- Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

- All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome. Currently, the concurrent audit shall be made in the form of maker checker which is done internally.

- The entire data and recordings of V-CIP shall be stored and the activity log along with the credentials of the official performing the V-CIP shall be preserved.

C. Risk Categorisation:

The Company has formulated an indicative list of customers, their respective risk categories and risk revision criteria by credit administration department which is attached as **Annexure-B.**

7. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

The Company shall obtain the following information/document 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:

From an individual, the Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time.

The Company shall carry out verification through Digital KYC as specified under Digital and Video KYC Process.

Such other documents including in respect of the nature of business and financial status of the customer, or an equivalent e-document of any OVD, the Company verify the digital signature as per provisions of IT Act, 2000 and any rules issued thereunder and take a live photo as specified under Digital and KYC Process.

The information collected from customers for the purpose of opening of account will be treated as confidential and details thereof will not be divulged for the purpose of cross selling, or for any other purpose without the explicit permission of the customer to the Company.

Provided PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained.

In case of Sole Proprietary firms for opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.
In addition to the above, any two of the documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained.

In cases where the company is satisfied that it is not possible to furnish two such documents, then company can accept only one of those documents as proof of business/activity. Provided company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Identification of Beneficial Owner:

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

(a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; **it is not necessary** to identify and verify the identity of any shareholder or beneficial owner of such entities.

(b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

The Identity, Address Proof and other documents required for Customer Due Diligence are attached and marked as **Annexure A.**

The Company shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any.

The database shall be subjected to periodic internal audit/inspection and shall be available for supervisory review.

8. ON – GOING DUE DILIGENCE

The Company shall undertake on-going due diligence of customers to ensure that the transactions are consistent with their knowledge about the customers, customers' business and risk profile, and the source of funds.

Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

The extent of monitoring shall be aligned with the risk category of the customer.

(a) A system of 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 shall be done.

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

9. PERIODIC UPDATION

Periodic updation of KYC documents needs to be done for following type of customers:

- High risk- at least once in every two years
- Medium risk- once in every eight years
- Low risk- once in every ten years

a) Individual Customers:

i. No change in KYC information:

In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter etc.

ii. Change in address:

- In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter, etc.

- The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

- Further, the Company at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.

iii. Accounts of customers, who were minor at the time of opening account, on their becoming major:

In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Company. Wherever required, the Company may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

b) Customers other than individuals:

i. No change in KYC information:

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

ii. Change in KYC information:

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

c. The company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, customers shall submit to the company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at companies end.

10. ENHANCED AND SIMPLIFIED DUE DILIGENCE PROCEDURE

- Accounts of non-face-to-face customers

The Company shall ensure that the first payment is to be affected through the customer's KYC complied account with another Company, for enhanced due diligence of non-face to face customers.

Aadhaar OTP based e-KYC in non-face to face mode has been permitted to be used for periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall, however, ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

Company shall verify the current address through positive confirmation before allowing operations in the account, PAN shall be obtained from the customer and shall be verified, customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP, etc.

- Accounts of Politically Exposed Persons (PEPs)

The Company generally does not establish any relationship with PEPs but it shall have the option of establishing a relationship with PEPs, the Company shall comply with RBI regulations.

- Client accounts opened by professional intermediaries

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

a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b) The Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c) The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Company, the Company shall look for the beneficial owners.
e) The Company shall, at its discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
f) The ultimate responsibility for knowing the customer lies with the Company.

11. RECORD MANAGEMENT

Records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules.
The Company shall,

- maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;
- preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during business relationship, for at least five years after the business relationship is ended;
- make available the identification records and transaction data to the competent authorities upon request;
- introduce a system of maintaining proper record of transaction prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit reconstruction of individual transaction, including the following:
  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.

e. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
f. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.
g. 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. If the same are not registered, the company shall register the details on the DARPAN Portal. The company shall also maintain such registration records for a period of five years after the business relationship between the customer and the RE has ended or the account has been closed, whichever is later.

12. REQUIREMENTS / OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS COMMUNICATIONS FROM INTERNATIONAL AGENCIES

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

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

The details of the two lists are as under:

i. The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

REs shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists

and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the REs for meticulous compliance.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated 104February 2, 2021.

Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 105February 2, 2021 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

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

Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

i. The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India.
ii. In accordance with paragraph 3 of the aforementioned Order, the company shall ensure not to carry out transactions in case the particulars of the individual /entity match with the particulars in the designated list.
iii. Further, company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
iv. In case of match in the above cases, company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to the State Nodal Officer, where the account / transaction is held and to the RBI. The company shall file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

v. The company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

vi. 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, REs shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

vii. In case an order to freeze assets under Section 12A is received by the company from CNO, the company shall, without delay, take necessary action to comply with the Order.

viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, a copy of application received from an individual/entity regarding unfreezing shall be forwarded by the company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

Jurisdictions that do not or insufficiently apply the FATF recommendations:

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

ii. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements. Explanation: The processes referred to in (a) & (b) above do not preclude a company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

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

Company is encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

13. KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer. The KYC information for sharing with CKYCR shall be in the prescribed template.

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

The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

The Company shall register itself on the Central Know Your Customer Registry ["CKYCR"] maintained by Central Registry of Securitisation and Asset Reconstruction and Security Interest of India ["CERSAI"] for the purposes of sharing KYC data.

The Company shall ensure that the KYC data is regularly shared / verified from the CKYCR.

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

The Company shall nominate two officers of the Company for the purpose of holding the roles of User Administrators. The two officers so appointed shall function in a manner wherein the maker checker concept amongst them is followed.

The Company will take following steps for the uploading:

i) CFPL will upload the KYC data pertaining to all individual accounts open on or after from April 01, 2017 and for Legal Entities from April 01, 2021 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

ii) It shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

iii) It will follow operational guidelines for uploading the KYC data which has been released by CERSAI.

iv) It shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for Individual and LEs as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

v) Once KYC identifier is generated by CKYCR, the Company shall ensure that the same is communicated to individual/LEs.

vi) The Company shall ensure that during the periodic updation, the customers are migrated to the current CDD standard.

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

- There is a change in the information of the customer as existing in the records of CKYCR.
- The current address of the customer requires to verify.
- If the Company considers, it is necessary 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.

KYC documents downloaded from the CKYCR, but **whose validity has lapsed**, are not used for KYC purpose.

KYC in case of Top – Up /Renewal:

In case of Top-up/Renewals, where KYC documents collected are not more than 12 months old, the Company will not strive to collect new KYC documents if there is no change in shareholding structure/partnership arrangement, change in authorised signatory of company/firm. In case of change, KYC documents of new beneficial owners/applicants/co-applicants/guarantors to be collected. In case of change in address, new address proof to be collected.

Self-Attestation Norms:

All documents should be self-attested by the applicant/co-applicant/guarantor to whom the document pertain.

In case where the documents run into more than 5 pages then self-attestation by the customer is required only in first and last page of the document.

For cases where documents are sent by the customer from his/her email ID registered with CFPL in application form, the documents would be considered as self-attested by the customer.

Unique Customer Identification Code:

- The Company shall assign a Unique Customer Identification Code ["UCIC"] to both existing as well as new customers, in order to link all account-based relationships/ transactions to the customer.
- KYC verification once done by one branch/office of the company shall be valid for transfer of the account to any other branch/office of the same company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

14. DIGITAL KYC PROCESS

a. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through his authenticated application of the Company.

b. 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 Log-in ID and Password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

c. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice-versa. The original OVD shall be in possession of the customer.

d. 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 shall put a watermark in readable form having CAF numbers, GPS Coordinates, authorized official name, unique employee code, and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the live captured photograph of the customer.

e. The Application of the Reporting Entities shall have the feature that only live photograph of the client is captured and no printed or video-graphed photograph of the client is captured. The background behind the client 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 client.

f. 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.

g. The live photograph of the client and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

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

i. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to client's own mobile number. Upon successful validation of the OTP, it will be treated as client signature on CAF. However, if the client 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 Reporting Entity shall not be used for client signature. The Reporting Entity must check that the mobile number used in client signature shall not be the mobile number of the authorized officer.

j. The authorized officer shall provide a declaration about the capturing of the live photograph of client 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 Reporting Entity. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

k. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Reporting Entity, 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 client for future reference.

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

m. On Successful verification, the CAF shall be digitally signed by authorized representative of the Reporting Entity 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.

15. REPORTING

The company shall furnish to the director, the Financial Intelligence Unit – India (FIU-Ind) information referred to in Rule 3 of PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. The company shall take note of reporting formats and comprehensive reporting formatting guide prescribed/released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in preparation of prescribed reports. The Company shall register on the FINnet portal, alongwith undertaking registration of the Principal Officer. The reports shall be filed by the Company online only. Any change in the Principal Officer shall be effected on the FINnet portal by the Company within one month of the date of such change. The Principal Officers of the company, where branches are not fully computerized, shall have a suitable arrangement to cull out the transaction details from branches which are not yet computerized.

The Company shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIU-Ind) and company shall communicate the name, designation, address and contact details of Designated Director and Principal Officer to the Reserve Bank. as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI at the following address alongwith necessary online filings. Illustrative List of Suspicious Transactions is attached herewith as **Annexure- C.**

16. CUSTOMER EDUCATION

Company shall educate Customers on the objectives of the KYC policy so that Customer understands and appreciates the motive and purpose of collecting such information. The Company shall prepare specific literature / pamphlets, terms and conditions etc. to educate the Customer about the objectives of this policy.

17. RELATIONSHIP PROOF

In order to establish relationship between applicant, co-applicant or guarantor below mentioned document should be obtained:

- Marriage Certificate
- PAN Card
- Birth Certificate
- Ration Card
- Valid Indian Passport
- Voters ID

- Aadhar Card

In the absence of any of the above-mentioned document's declaration for relationship proof should be obtained.

Type of relationships eligible under the definition of "relative" will be as follows:

- Spouse
- Father
- Mother
- Brother
- Unmarried sister
- Child

18. INTRODUCTION OF NEW TECHNOLOGIES

Companies shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and preexisting products.

Further, REs shall ensure:

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

19. SECRECY OBLIGATIONS AND SHARING OF INFORMATION:

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

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

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

(d) The exceptions to the said rule shall be as under:
   i. Where disclosure is under compulsion of law
   ii. Where there is a duty to the public to disclose,

iii. the interest of RE requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

20. Hiring of Employees and Employee Training

(a) An adequate screening mechanism, including the Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

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

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

21. Uploading documents on Third Party platform

CFPL shall upload the KYC and/or other documents of borrower, authorised signatory/ies, guarantor/s and service providers on third party platform (for e.g. "leegality") for execution and/or attestation purpose.

22. Review

A review shall be done every year.

For any clarification RBI circular/notification shall be referred to.

Annexure-A

Particulars	Constitution						
	Company	**Partnership Firm/LLP**	**Proprietorship Firm**	**HUF**	**Trust/Societies**	**Individual/ Authorised Signatory**	**BOI/ Unincorporated Association**
Identity Proof	**All**	**All**	**All**	**All**	**All**	**All**	**All**
	PAN	PAN of firm or LLP	PAN of Proprietor	PAN of HUF, Karta & all Co-Parceners	PAN	PAN	PAN
	MOA	Partnership Deed/ LLP Agreement	-	-	Trust Deed	-	-
	AOA	-	-	-	Articles of society	-	-
	COI	Registration Certificate	Registration certificate (MSME or Udyam/ GST certificate/Shop & Estb. Certificate/Sales and income tax returns	Registration certificate (MSME or Udyam/ GST certificate)	Registration Certificate under Trust/ Society Act	-	-
Address Proof for registered office and principal place of business if its different	**Any 1**	**Any 1**	**Any 1**	**Any 1**	**Any 1**	**Any 1 each for identity and address proof**	**Any 1**
	*Utility Bill not older than 2 months with Rent Agreement (if Rental Premises)	*Utility Bill not older than 2 months with Rent Agreement (if Rental Premises)	*Utility Bill **OR** Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)	*Utility Bill not older than 2 months with Rent Agreement (if Rental Premises)	*Utility Bill not older than 2 months with Rent Agreement (if Rental Premises)	Passport / Driving License / Voters ID Card / Aadhar Card / Municipal Tax receipt (if address is not updated then utility bill or bank statement is acceptable for 3 months)	*Utility Bill not older than 2 months with Rent Agreement (if Rental Premises)
	Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)	Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)	Registration certificate (MSME or Udyam/ GST certificate/Shop & Estb. Certificate/Sales and income tax returns	Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)	Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)		Bank Statement not older than 2 months with Rent Agreement (if Rental Premises)
***Acceptable utility Bill - Electricity / GAS Pipeline / Postpaid Landline or Mobile / Water**							

	Constitution						
Particulars	**Company**	**Partnership Firm/LLP**	**Proprietorship Firm**	**HUF**	**Trust/Societies**	**Individual/ Authorised Signatory**	**BOI/ Unincorporated Association**
Compulsory Documents	**All**	**All**	**All**	**All**	**All**	**All**	**All**
	List of Shareholders and relevant persons holding senior management position on letterhead (Require KYC of shareholder, if shareholding is more than 10% of total shareholding or exercise control through other means)	List of Partners on letterhead (Require KYC of partner/s, who has/have ownership/entitlement to more than 15% of capital or profits of the partnership)	Sole Proprietorship Declaration	List of Co-Parceners	List of beneficiaries,Trustees,settlor and authors on letterhead (Require KYC of trustees & persons authorised to transact on behalf of the trust and beneficiaries who are having 10% or more interest in the trust and any other natural person who exercise ultimate control over the trust)	-	List of Members on letterhead (Require KYC of beneficiary (natural person), has/have ownership/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals)
	LEI Code (If exposure is 25 crores or more)	LEI Code (If exposure is 25 crores or more)	LEI Code (If exposure is 25 crores or more)	LEI Code (If exposure is 25 crores or more)	LEI Code (If exposure is 25 crores or more)	-	LEI Code (If exposure is 25 crores or more)
	Approval resolution from the Board and/or Shareholders and resolution pertaining to the authorisation given to signing persons	For Partnership- Partnership Authority Letter For LLP - Approval resolution from the Partners and resolution pertaining to the authorisation given to signing persons Note - Not required if all partners are signing the loan related documents	-	Resolution/ Authority Letter	Resolution of Trust/Society	-	Resolution/ Authority Letter
	List of Directors	-	-	-	-	-	-
	Photograph of authorised signatory/ies	Photograph of authorised signatory/ies	Photograph of authorised signatory/ies	Photograph of authorised signatory/ies	Photograph of authorised signatory/ies	Photograph of individual/ authorised signatory	Photograph of authorised signatory/ies

Note: Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.

ANNEXURE- B

CRITERIA FOR DETERMINATION OF RISK

Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

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

Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of the company which as mentioned below:

High Risk- Category A Customers

1. Non-Resident Customers (NRIs)
2. Politically Exposed Persons (PEP) of Indian / Foreign origin
3. Trustees, Charities, NGOs/NPOs (especially those operating on a cross border basis)
4. Unregulated clubs and organisations receiving donations (excluding NGOs/NPOs promoted by United Nations or its agencies)
5. Complex business ownership structures (which can make it easier to conceal underlying
6. Beneficiaries where there is no legitimate commercial rationale
7. Shell Companies (which have no physical presence in the country in which it is incorporated)
8. The existence simply of a local agent or low-level staff does not constitute physical presence
9. Partnership firms with sleeping partners
10. Person with dubious reputation as per public information available
11. Dealers in high value or precious goods e.g., bullion dealers, gems, jewels
12. Real Estate developers/agents
13. Casinos and other gambling business
14. Capital Market (Share Brokers, Investment Management Companies etc.)
15. Arms & Ammunition manufacturers and dealers
16. Multi-level marketing companies

Medium Risk- Category B Customers

1. Salaried applicant with variable income/ unstructured income receiving Salary in cheque
2. Salaried applicant working with Private Limited Companies, Proprietary, Partnership firms
3. Self- employed professionals other than High Net-Worth Individuals
4. Self-employed customers with sound business and profitable track record for a reasonable period
5. HNIs with an occupation track record of more than 3 years.

Low Risk – Category C Customers

Low Risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories. Customer carrying low risk may include the following:

1. Salaried employees with well-defined salary structures for over 5 years
2. People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies etc. In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company will obtain approval from Board of Directors in such cases to continue the business relationship with such person, and also undertake enhanced monitoring.
3. People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
4. People working with Public Sector Units, People working with reputed Public Limited Companies and Multinational Companies.

Risk Revision Criteria by Credit Administration Department

Particulars	Risk Category for KYC
Both the documents are available (identity proof and address proof)	Low
Either of the document not available	High

ANNEXURE- C

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS

Suspicious Activities Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash rather than normally associated with the normal commercial operations of the company, e.g. cheques.

Transactions that do not make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customers furnish a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

Accounts with a large volume of credits whereas the nature of business does not justify such credits.

Attempts to avoid Reporting/Record-keeping Requirements

- A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

- Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.

An account where there are several cash transactions below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer/Client who provides Insufficient or Suspicious Information

- A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
- A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

- A customer who has no record of past or present employment but makes frequent large transactions.

Employees arousing Suspicion

- An employee whose lavish lifestyle cannot be supported by his or her salary.
- Negligence of employees/wilful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored:

- Large Cash Transactions
- Multiple accounts under the same name
- Placing funds in term Deposits and using them as security for more loans
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts