THE

KNOW YOUR CUSTOMERS (KYC) AND PREVENTION OF MONEY LAUNDERING (PML) POLICY

OF

ABHIYAN CAPITAL (INDIA) PRIVATE LIMITED

(Formerly Dowell Fiscal Services Private Limited)

CIN: U65999MH1995PTC289390

This Policy has been approved by the Board of Directors of Abhiyan Capital (India) Private Limited and shall remain effective until amended, revised, or superseded by the Board of Directors.

KNOW YOUR CUSTOMERS (KYC) AND PREVENTION OF MONEY LAUNDERING (PML) POLICY

Abhiyan Capital (India) Private Limited
(Formerly Known as Dowell Fiscal Services Private Limited)

EXECUTIVE SUMMARY

The primary objective of the "Know Your Customer" (KYC) Policy is to prevent Abhiyan Capital (India) Private Limited (ACIPL) from being used, intentionally or otherwise, by unscrupulous elements for fraudulent, money laundering, and terrorist financing activities, as enunciated in the "Customer Acceptance Policy" of ACIPL and various circulars issued by the Reserve Bank of India (RBI) on the subject matter from time to time. KYC procedures also enable us to know and understand customers and their financial dealings better, which, in turn, helps us manage their risks prudently.

The Customer Acceptance Policy shall not result in the denial of financial services to any person, including financially or socially disadvantaged persons and Persons with Disabilities (PwDs). No onboarding or KYC updation request shall be rejected without recording the reasons in writing by the authorized officer after due application of mind.

1. INTRODUCTION

This Policy has been drafted in accordance with the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, issued by the Reserve Bank of India, the Prevention of Money-Laundering Act, 2002, and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. The Policy incorporates the Standard Operating Procedures (SOPs) relating to Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements and sets out the framework for compliance with the applicable regulatory and statutory obligations (hereinafter referred to as the "KYC Policy").

IMPORTANT TERMS & DEFINITIONS

A. Applicability - All Branches/Offices/authorized officers shall mandatorily comply with the procedures laid down in this Policy. Non-compliance will be construed as misconduct on the part of the employee, which will attract appropriate penal action.

B. Transactions - The Policy will be applicable to all "Transactions" undertaken by the Company. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery, or the arrangement thereof and includes:

a. opening of a loan account;
b. deposit, withdrawal, exchange, or transfer of funds in any currency, whether in cash or by cheque, payment order, or other instruments, or by electronic or other non-physical means;

c. entering into any fiduciary relationship;
d. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
e. establishing or creating a legal person or legal arrangement.

C. Customer - The Policy will be applicable to all "Customers", including Applicants, Co-Applicants, Guarantors, Beneficial Owners (BOs), and Business Partners. "Customer" means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person engaged in the transaction or activity is acting. Customer will include the following:

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person not falling within any one of the above persons (a to e), and
g. any agency, office, or branch owned or controlled by any of the above persons (a to f).

KYC documentation collection, validation, and OSV (Original Seen & Verified) check/certification, as specified in this circular, shall be fulfilled either in physical form, through V-CIP (Video Customer Identification Process), or in digital mode.

D. Beneficial Ownership – Beneficial Ownership – Identification of Beneficial Owner(s) shall be carried out in accordance with the RBI Master Direction – KYC. The beneficial owner shall be identified as follows: (i) Company – the natural person(s) having controlling ownership interest of more than 10% of the shares, capital, or profits, or exercising control through other means; (ii) Partnership Firm – the natural person(s) having ownership of or entitlement to more than 10% of the capital or profits of the partnership, or exercising control through other means; (iii) Unincorporated Association/Body of Individuals – the natural person(s) having ownership of or entitlement to more than 15% of the property, capital, or profits of such association/body; and (iv) Trust – the author of the trust, trustee(s), beneficiaries having 10% or more interest in the trust, and any other natural person exercising ultimate effective control over the trust shall be identified as beneficial owner(s).

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

F. 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.

G. Where equivalent e-documents are obtained, the Company shall verify the digital signature in accordance with the Information Technology Act, 2000.

2. APPOINTMENT OF PRINCIPAL OFFICER (PO)

As required under the Prevention of Money Laundering Act, 2002 (PMLA), Mr. Pankaj Jain has been appointed as the Principal Officer of the Company. The Principal Officer shall, inter alia, be responsible for ensuring compliance with the applicable AML/CFT framework, monitoring transactions, and reporting and sharing information as required under the Prevention of Money Laundering Act, 2002, the rules framed thereunder, and other applicable regulations, as amended from time to time. The name, designation, address, and contact details of the Principal Officer shall be communicated to the Financial Intelligence Unit – India (FIU-IND) and the Reserve Bank of India (RBI) by the Compliance/Secretarial Department in accordance with applicable regulatory requirements.

The Legal and Compliance Department shall separately notify the Principal Officer of his roles and responsibilities under the KYC and AML framework.

3. APPOINTMENT OF DESIGNATED DIRECTOR

As required under RBI guidelines, Mr. Rohit Tiku has been appointed as the Designated Director for ensuring compliance with the obligations under the PML Act. The name, designation, address, and contact details of the Designated Director shall be communicated to FIU-IND and the Reserve Bank of India (RBI) by the Compliance/Secretarial Department in accordance with applicable regulatory requirements.

4. COMPLIANCE OF KYC POLICY

4.1 CONSTITUTION OF SENIOR MANAGEMENT

As per the RBI circular, the Senior Management has been constituted for the KYC Policy. Senior Management shall comprise Whole-Time Directors, the Chief Financial Officer, the Chief Operating Officer, the Chief Business Officer, and the Head of Credit and Risk.

The responsibility shall be for the effective implementation of policies and procedures within their respective departments. Pursuant to this clause, the Legal and Compliance Department shall separately notify the Senior Management of its roles and responsibilities under the KYC Policy.

4.2 CONCURRENT/INTERNAL AUDIT

An independent evaluation of the compliance functions pertaining to KYC and PMLA shall be conducted. It shall include verification of compliance with KYC/AML policies and procedures (both design and implementation) on a quarterly basis and highlight the necessary modifications, if any, so as to ensure compliance. A compliance report on the KYC Policy shall be submitted to the Audit Committee/Board on a quarterly basis.

4.3 OUTSOURCING

The decision-making function of determining compliance with KYC norms shall not be outsourced.

4.4 HIRING AND TRAINING

The Human Resources Department shall put in place a screening mechanism as an integral part of its personnel recruitment/hiring process. The HR, Legal & Compliance, and Operations Departments shall arrange an ongoing employee training program for different categories of staff and ensure that they are adequately trained in KYC/AML procedures. 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 a lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulations, and related issues shall be ensured.

4.5 CUSTOMER DUE DILIGENCE

Customer due diligence means identifying and verifying the customer and Beneficial Owner using "Officially Valid Documents" as proof of identity and proof of address.

4.6 CENTRAL KYC RECORDS REGISTRY

CKYCR means an entity that receives, stores, safeguards, and retrieves the KYC records of customers in digital form. The Operations Department has taken the necessary steps to comply with the norms of CKYCR within the specified timelines. The Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) to act as, and perform the functions of, the CKYCR.

4.7 REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)

Under FATCA and CRS, the Finance Department shall adhere to the provisions of the Income Tax Rules and accordingly take steps to comply with the reporting requirements:

- Registration shall be done on the URL https://incometaxindiaefiling.gov.in for filing returns. E-filing reports shall be submitted using the digital signature of the Designated Director by uploading either Form 61B or a NIL report, for which the scheme prepared by the Central Board of Direct Taxes (CBDT) shall be referred to.

- Reference may be taken from www.fedai.org.in/revaluationrate.aspx for carrying out due diligence procedures for the purpose of identifying reportable accounts under Section 114H of the Income Tax Rules.

- The IT framework shall be utilized for due diligence and for recording and maintaining information.

- The Senior Management, constituted under the Designated Director, shall ensure compliance with updated instructions, rules, guidance notes, and press releases issued by the Central Board of Direct Taxes (CBDT) from time to time and available on the website http://www.incometaxindia.gov.in/Pages/default.aspx.

• The Company may take note of the following:

i. Updated Guidance Note on FATCA and CRS;

ii. A press release on 'Closure of Financial Accounts' under Rule 114H(8).

4.8 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT (ML/TF/PF)

The Company shall periodically undertake a documented ML/TF/PF Risk Assessment exercise covering customers, products, geographies, delivery channels, transaction types, and business relationships. The assessment shall be reviewed at least annually and placed before the Board/Risk Management Committee.

5. THE KYC POLICY INCLUDES THE FOLLOWING KEY ELEMENTS:

5.1 Customer Acceptance Policy - The Customer Acceptance Policy shall not result in the denial of financial services to any person, including financially or socially disadvantaged persons and Persons with Disabilities (PwDs). No onboarding or KYC updation request shall be rejected without recording reasons in writing by the authorized officer after due application of mind.

5.2 Customer Identification Procedures (CIP) – (1) Physical, (2) Video – CIP, (3) Digital – KYC

5.3 Risk Management - Risk categorization and the underlying rationale shall remain confidential and shall not be disclosed to the customer to avoid tipping-off.

5.4 Customer Due Diligence (CDD) procedure as specified in Annexures

5.5 Monitoring of Transactions

5.6 Business Partner Due Diligence

5.7 Annexures

5.1 CUSTOMER ACCEPTANCE POLICY

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

(b) No account is opened where the Company is unable to apply appropriate Customer Due Diligence measures (CDD), either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

(c) Where the Company forms a suspicion of money laundering or terrorist financing and reasonably believes that carrying out the CDD process may tip off the customer, the Company may discontinue the CDD process and file an STR with FIU-IND.

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

(e) The mandatory information to be sought for KYC purposes while opening an account and during periodic updation shall be as specified in this procedure note.

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

(g) The CDD procedures are applied at the Unique Customer Identification Code (UCIC) level.

(h) The CDD procedure is followed for all joint account holders while opening a joint account.

(i) The de-duplication check should ensure that the identity of the customer does not match with any person or entity whose name appears in the sanctions lists circulated by the Reserve Bank of India. The de-duplication database should be updated periodically by the Compliance and IT Teams.

(j) The Company shall maintain appropriate systems for screening customers against applicable sanctions lists, including UNSC sanctions lists, domestic watchlists, terrorist lists, and any other regulatory lists prescribed from time to time.

(k) Where GST details are available for the customer/entity, the GST number shall be verified through the search/verification facility of the issuing authority.

(l) Where PAN is obtained from the customer, the same shall be verified through the verification facility/database of the issuing authority.

5.1.1 KYC PROCESS

CUSTOMER IDENTIFICATION

Every employee of ACIPL or an ACIPL authorized representative, as specified in the respective product policies such as Dealer/DSA/other representatives, shall establish a customer relationship only after the identity and address of the customer and all those who represent the customer have been verified and found satisfactory. The Company can also utilize manual/digital/electronic mechanisms for validating the name and address of the customer.

Step 1

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

Step 2

The customer is required to complete the Application Form/Request for Loan in physical/digital form, wherein details on the background and facilities opted for by the customer are recorded. All applicable fields should be completed.

Step 3

The details furnished in the Application Form – Physical/Digital shall be supported by a photograph (applicable in the case of an individual), proof of identity, and proof of address. The documents that can be accepted to support the identity and address of all parties signing the agreement, i.e., applicant, co-applicant, guarantor, and Beneficial Owner (BO), are listed

in the attached Annexure A2 – List of Important Instructions, Documents Accepted as OVD (Officially Valid Document) – Proof of Identity and Proof of Address. OVDs are collected to identify customers and confirm their stay at a particular address with the help of reliable, independent source documents, data, or information. The photograph should be a recent colour passport-size photograph and can be physical or digital.

Step 4

Supporting documents obtained shall be verified with the originals and certified by the person verifying them as a 'True Copy', i.e., Original Seen and Verified (OSV). The ACIPL employee or ACIPL representative who meets the customer should perform the verification (OSV stamp with name, signature, and employee/representative code). The same can be done in physical or digital mode.

Step 5

The de-duplication check with the ACIPL group system should be conducted. The necessary de-duplication check is to be carried out before opening a new account, as well as to ensure, as far as possible, that the identity of the applicant does not match with any person having a known criminal background, willful defaulters as per the list published by the RBI, or banned entities such as individual terrorists, terrorist organizations, or the list of individuals and entities approved by the Security Council Committee established pursuant to various United Nations Security Council Resolutions (UNSCRs), etc. The de-duplication check (Internal Dedupe) should be mandatorily conducted.

Step 6

Wherever required, verification of customer information through various means, such as tele-verification/contact point verification, may be conducted by an ACIPL employee or an ACIPL authorized representative.

5.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

5.2.1 Customer Identification Procedure (CIP) - Physical

1. The Company shall undertake identification of customers in the following cases, as and when applicable:

   (a) Commencement of an account-based relationship with the customer.

   (b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

   (c) When there is doubt about the authenticity or adequacy of the customer identification data obtained.

   (d) Selling third-party products as agents, selling their own products, payment of dues of credit cards, sale and reloading of prepaid/travel cards, and any other product for more than rupees fifty thousand.

(e) Carrying out transactions for a non-account-based customer, i.e., a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When the Company has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(g) The Company shall ensure that introduction is not sought while opening accounts.

2. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company shall, at its option, rely on customer due diligence carried out by a third party, subject to the following conditions:

(a) Records or information relating to the customer due diligence carried out by the third party are obtained within two days from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by the Company to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available by the third party upon request without delay.

(c) The third party is regulated, supervised, or monitored and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, shall remain with the Company.

5.2.2 Re-use of KYC is allowed only for Low and Medium Risk Customers, provided:

I. Customer consent is obtained for the re-use of the existing KYC documents.

II. The old KYC documents available are valid and comply with the applicable KYC Policy as on the date of fresh login of the case.

III. There is no change in address or customer identification.

IV. The address mentioned in the Application Form for the proposed funding matches the downloaded KYC document.

V. A declaration shall be provided by the ACIPL employee stating that the KYC has been downloaded from DMS. The employee downloading the document shall sign all KYC documents mentioning his/her name, employee ID, and date.

VI. If the KYC has been pre-written by the customer for restricted use, then fresh KYC shall be collected.

VII. In case the contact point verification/customer interaction report indicates that the customer address/KYC details do not match the downloaded KYC, then fresh KYC shall be obtained.

VIII. Additionally, in the case of Non-Individual customers, the following documents are required afresh from the customer/digital source:

▪ Company – Board Resolution, List of Directors, Latest Shareholding Pattern, Power of Attorney (if applicable).

▪ Partnership Firm – Partnership Deed/List of Partners with Profit Sharing Ratio, Partnership Authority Letter, Power of Attorney (if applicable).

▪ HUF – HUF Letter.

▪ AOP/BOI (including Trust, Society, etc.) – List of members with beneficial interest percentage, Resolution as per entity type, and Power of Attorney (if applicable).

5.2.3 Video - Customer Identification Procedure (V-CIP / Video - KYC)

V-CIP is an alternate digital process laid down to complete the KYC requirement of an individual customer, as compared to the Physical Customer Identification Process, to gather information and documents required for Customer Due Diligence (CDD) purposes. This is also called Video-KYC. Such a process shall be treated as equivalent to a face-to-face physical process. The V-CIP shall follow standard process steps, controls, and design requirements.

Sr.	Parameters	Norms
1.	Applicability	**Individual** • Live V-CIP is applicable for individuals. **Non-Individual** • Proprietors in the case of proprietorship firms, along with the e-document of business activity proof as defined in CDD norms. • For other non-individual entity customers, Live V-CIP shall be applicable for authorized signatories and BO customers. • Updation/periodic updation of KYC of eligible customers.
2.	Customer Consent	Explicit customer consent is required before V-CIP is undertaken.
3.	Execution of V-CIP	An official of the ACIPL Group shall carry out the live V-CIP process with the customer.
4.	PAN Verification	A clear image of the PAN Card/e-PAN shall be captured while the customer displays it during V-CIP.• Mandatory PAN verification shall be conducted from the government data source through a suitable vendor API.
5.	Recording of Video & Photograph	The employee shall record the video and capture a live photograph/snapshot of the customer present for V-CIP.

6.	Video Recording Quality and Geo-Tagging	The video recordings should contain the live GPS coordinates (geo-tagging) of the customer undertaking the V-CIP and a date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
7.	Face Liveliness	The V-CIP application shall have components for face liveness, spoof detection, as well as face-matching technology with a high degree of accuracy. The Company will use advanced technology, including artificial intelligence, for various matching processes (such as facial matching, etc.) to ensure the integrity of V-CIP. Notwithstanding the above, the final responsibility for customer identification shall rest with the Company.
8.	Customer Identification through Aadhaar XML Verification	Offline Aadhaar verification shall be required during V-CIP. The Aadhaar XML and secure code should not be more than three days old from the date of V-CIP. If an image of the Aadhaar document is stored, the Aadhaar number should be blacked out/redacted. The address on Aadhaar should match the current address of the customer; otherwise, normal physical KYC can be executed unless functionality is developed in the system to capture the prescribed additional document as proof of the current address.Further, once system capability is developed, the following other methods of customer identification may be executed: KYC records downloaded from CKYCR using the KYC identifier provided by the customer; or Equivalent e-documents of Officially Valid Documents (OVDs), including documents issued through Digi Locker.
9.	Photo Match	The live photo captured during V-CIP should match the photo retrieved from PAN and Aadhaar authorities through digital mode. The matching algorithm shall provide a matching percentage, and the employee shall confirm the photo match. The threshold for photo matching shall be decided by Risk and RCU and modified from time to time based on learnings.
10.	Name Matching Logic	Name-matching logic shall be inbuilt in the system between the name received from the PAN API and Aadhaar XML.
11.	Security Questions	In order to conduct a liveliness check of the customer during V-CIP, the employee shall ensure that the sequence and/or type of questions are varied to establish that the interactions are real-time and not pre-recorded.

12.	V-CIP De-duplication Check	The system shall identify whether the V-CIP customer is an existing or new customer, whether the case was rejected earlier, or whether the name appears on any negative list. Such cases should be rejected.
13.	Concurrent Audit	Concurrent audit shall be mandatory for the completion of each V-CIP. The audit shall be conducted by an employee from a different department, as decided by management from time to time, such as Operations, CPC, RCU, etc.
14.	IT Security	The V-CIP shall be a seamless, real-time, secure, end-to-end encrypted audio-visual interaction with the customer, and the quality of communication shall be adequate to allow identification of the customer beyond doubt. The system should be robust enough to guard against spoofing and any other fraudulent manipulation.• Software security audits and validation shall be conducted before launch by the competent authority.• A minimum baseline cyber security and resilience framework shall be prepared by the IT Department and updated from time to time, along with other general guidelines on IT risks.
15.	Company Domain	The technology infrastructure should be housed on the Company's own premises/secured infrastructure, and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Where a cloud deployment model is used, ownership of the data shall remain with ACIPL, and video recordings shall not be retained by the cloud service provider or third-party technology provider assisting the Company in V-CIP. The audio-visual interaction shall be triggered from the Company's own domain and not from a third-party service domain. The recorded video shall be stored in safe and secure custody with a date and time stamp. Technology outsourcing for V-CIP shall be governed by applicable RBI guidelines issued from time to time.
16.	Data Encryption	The V-CIP system shall ensure end-to-end encryption of data between the customer's device and the hosting point of the V-CIP application, as per appropriate encryption standards. Customer consent should be recorded in an auditable and tamper-proof manner.
17.	Control on IP	The V-CIP infrastructure/application should be capable of preventing connections from IP addresses outside India or from spoofed IP addresses.

18.	System Testing	The V-CIP system shall undergo necessary tests such as Vulnerability Assessment, Penetration Testing, and Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gaps reported under this process shall be mitigated before implementation is rolled out. The test certificate shall be recorded and retained for future reference from the competent authority.
19.	Audit Trail	The activity log, along with the credentials of the official performing the V-CIP, shall be recorded and preserved.
20.	Clear Workflow	A clearly documented workflow incorporating all regulatory requirements shall be established for carrying out V-CIP.
21.	Reporting of Fraud under RBI Guidelines	Any case of forged identity through V-CIP shall be reported as a cyber security event under the extant regulatory guidelines.
22.	Employee Training	All employees engaged in executing V-CIP and conducting concurrent audits shall be trained by the department responsible for V-CIP. Employees should be capable of carrying out liveliness checks and detecting any fraudulent manipulation or suspicious conduct by the customer and acting upon it. Any prompting observed by the employee at the customer's end shall lead to rejection.
23.	V-CIP Failure	If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated. If, for any reason, V-CIP fails or yields a negative outcome, the normal physical customer identification process shall remain available for execution. The employee executing the V-CIP or the concurrent auditor shall record the reason for the failure of V-CIP if that stage is reached. There may be technical reasons for the failure or non-execution of V-CIP.
24.	V-CIP Data and Video Storage	The entire data and recordings of V-CIP shall be stored in a safe and secure manner and shall bear a date and time stamp that facilitates easy historical data retrieval.

5.2.4 Digital KYC

Digital KYC means capturing a live photograph of the customer and OVD/proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photograph is being taken by the Company employee. The prerequisite norms for executing the Digital KYC facility are as follows:

1. The Company is required to have a Digital Application to execute the Digital KYC process with the customer.

2. Access to 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 a login ID and password, Live OTP, or Time OTP-controlled mechanism provided by the Company to its authorized officials.

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

4. The Company must ensure that a live photograph of the customer is taken by the authorized officer and that the same photograph is embedded in the Customer Application Form (CAF). Further, the Company's system application shall place a watermark in readable form containing the CAF number, GPS coordinates, authorized official's name, unique employee code (assigned by the Company), and date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

5. The Company's application shall have the feature whereby only a live photograph of the customer is captured and no printed or videographed photograph of the customer is accepted. The background behind the customer while capturing the live photograph should be white in colour, and no other person shall appear in the frame while capturing the live photograph of the customer.

6. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar, where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above, and watermarking in readable form as mentioned above shall be applied. There shall be no skew or tilt in the mobile device while capturing the live photograph of the original documents.

7. The live photograph of the customer and the original documents shall be captured in proper lighting so that they are clearly readable and identifiable.

8. Thereafter, all entries in the CAF shall be completed based on the documents and information furnished by the customer. In documents where a Quick Response (QR) code is available, such details may be auto-populated by scanning the QR code instead of manually filling in the details. For example, in the case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where a QR code is available, details such as name, gender, date of birth, and address may be auto-populated by scanning the QR code available on the Aadhaar/e-Aadhaar. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text "Please verify the details filled in the form before sharing the OTP" shall be sent to the customer's own mobile number. Upon successful validation of the OTP, it shall be treated as the customer's signature on the CAF. However, if the customer does not have his/her own mobile number, then the mobile number of a family member/relative/known person may be used for this purpose and shall be clearly mentioned in the CAF. In any case, the mobile number of an authorized officer registered with the Company shall not be used for

customer signature. The RE must ensure that the mobile number used for customer signature is not the mobile number of the authorized officer.

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

10. Subsequent to all these activities, the Application shall provide information regarding the completion of the process and submission of the activation request to the activation officer of the Company and shall also generate a transaction ID/reference ID for the process. The authorized officer shall intimate the transaction ID/reference ID to the customer for future reference.

11. The authorized officer of the Company shall check and verify that:

    (i) the information available in the document image matches the information entered by the authorized officer in the CAF;

    (ii) the live photograph of the customer matches the photograph available in the document; and

    (iii) all necessary details in the CAF, including mandatory fields, are properly completed.

12. Upon successful verification, the CAF shall be digitally signed by the authorized officer of the Company, who shall take a printout of the CAF, obtain the signature/thumb impression of the customer at the appropriate place, and then scan and upload the same into the system. The original hard copy may be returned to the customer.

5.2.5 CKYCR

CKYCR is an entity under CERSAI that receives, stores, safeguards, and retrieves KYC records of customers in digital form. CKYCR manages KYC records for both Individuals and Legal Entities.

Sharing of Information with CKYCR

• Operations shall upload the KYC records of customers within 10 days of the commencement of an account-based relationship, such as booking of a contract.

• Applicable operational guidelines issued by CERSAI for uploading KYC data shall be followed.

• The KYC records of Individuals and Legal Entities shall be uploaded to CKYCR for accounts opened on or after 01.04.2017 and 01.04.2021, respectively.

• The KYC Identifier generated by CKYCR shall be communicated to the Individual or Legal Entity, as applicable.

• The CKYCR Identifier generated after submission of KYC is required to be communicated to the respective customer.

• Periodic updation of KYC information/documents received for Individuals and Legal Entities shall be carried out for periods prior to and after the above-mentioned dates.

• During periodic updation, customers shall be migrated to current CDD standards (KYC documentation and information).

Use of Information from CKYCR

With the explicit consent of the customer and submission of the KYC Identifier by the customer, or through acceptable digital solutions, the Company shall retrieve/download KYC records online from CKYCR using the KYC Identifier. In such cases, the customer shall not be required to submit KYC/OVD documents, information, or any additional identification document or detail, subject to the following conditions:

i. This provision is applicable only to customers falling under the Low Risk or Medium Risk category.

ii. There is no change in the customer's information (such as identification details, address, or other personal information) as recorded in CKYCR.

iii. The address as per the application form and CKYC documents is the same. Additionally, wherever FI is conducted, the FI should confirm the same address.

iv. The acceptable vintage of CKYC documents used shall be defined by the Risk Department from time to time.

v. The document should be valid at the time of the proposed loan, and it should be an acceptable KYC document as per the Policy.

vi. If, for any specified reason, the customer is selected for additional/enhanced due diligence, then the customer's identity and address shall be verified through appropriate means, which may include submission of additional KYC documents and a personal visit.

vii. In case contact point verification/customer interaction reports indicate that the customer's address/KYC details do not match the downloaded KYC, then fresh KYC shall be obtained.

viii. Additionally, in the case of non-individual customers, the following documents are required afresh from the customer/digital source:

▪ Company – Board Resolution, List of Directors, Latest Shareholding Pattern, Power of Attorney (if applicable).

▪ Partnership Firm – Partnership Deed/List of Partners with Profit Sharing Ratio, Partnership Authority Letter, Power of Attorney (if applicable).

▪ HUF – HUF Letter.

▪ AOP/BOI (including Trust, Society, etc.) – List of members with beneficial interest percentage, Resolution as per entity type, and Power of Attorney (if applicable).

5.3 RISK MANAGEMENT

5.3.1 CUSTOMER SCREENING

The risk assessment procedure begins with screening against Negative/Freeze Lists. Upon receipt of any caution lists issued by the Reserve Bank of India to the Legal/Compliance Department, the same shall be provided to the IT Department by the Business Intelligence Department for uploading into the Internal Dedupe Database. The procedure for screening of lists is as follows:

(i) The Internal Dedupe Database shall be enhanced with various lists to screen the name, date of birth, and/or other relevant data of the customer.

(ii) Where information is obtained that an existing customer or the Beneficial Owner of an existing account has subsequently become a PEP, whether through information available in the public domain or through customer interaction at a branch or during account servicing, senior management approval shall be required to continue the business relationship, and the account shall be subject to enhanced CDD measures.

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

ACIPL shall not allow the opening and/or holding of an account on behalf of a client by professional intermediaries, such as lawyers, chartered accountants, etc., who are unable to disclose the 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 ACIPL's ability to know and verify the true identity of the client on whose behalf the account is held, determine the beneficial ownership of the account, or understand the true nature and purpose of the transaction(s), shall not be permitted to open an account on behalf of a client.

It should also be noted that information collected from the customer for the purpose of opening an account should be kept confidential and not disclosed for cross-selling or any other purpose. Any additional information required from the customer shall be sought separately.

5.3.2 CUSTOMER RISK CATEGORIZATION

Risk Profile

As per the Company's "Know Your Customer (KYC) and Anti-Money Laundering Measures" Policy, customers shall be categorized as Low Risk, Medium Risk, High Risk, or Unacceptable based on their risk profile.

Process of Risk Profiling

For risk management purposes, the Company follows a risk-based approach after taking into consideration its assessment and risk perception. Each customer is categorized as Low Risk, Medium Risk, or High Risk.

In this note, the term "risk" is considered in the context of money laundering and terrorist financing and not credit risk, loan default risk, or similar risks.

Risk profiling of customers is based on the customer's identity, social and financial status, nature of business activity, information regarding the customer's business, location, etc. While assessing customer identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be considered.

5.4 CUSTOMER DUE DILIGENCE (CDD) MEASURES

CDD measures are applied based on the risk profile of the customer. The risk ratings and the related due diligence measures are summarized below:

Risk Profile	Due Diligence Measures
Low & Medium Risk	Standard Measures
High Risk	Enhanced Measures

5.4.1 Process for Customer Risk Categorization

1. The relevant section specifying the Risk Category of the customer should be completed.
2. Risk categorization of customers into Low Risk (Category A), Medium Risk (Category B), and High Risk (Category C) shall be carried out based on the information available.
3. For customers categorized as “High Risk (Category C)”, enhanced due diligence as specified below is mandatory:

   (a) An ACIPL employee shall visit the customer's premises to ascertain the actual existence of the business/industrial unit or assess the financial status of the person and verify that the scale of operations is commensurate with the declared turnover.

   (b) The case shall be approved, upon recommendation from the Head of Business, jointly by the Head Credit/National Credit Manager and the Risk Head/Chief Risk Officer after reviewing the customer visit report, financial documents, and source of funds.

   (c) Operations shall ensure that no disbursement is made unless the Risk Categorization has been completed.

   (d) Operations shall also ensure that the requisite approvals for customers classified as High-Risk are available.

   (e) Operations shall ensure that the correct risk categorization is updated in SAP.

4. It should be noted that the customer profile is a confidential document, and the details contained therein shall not be divulged for any other purpose. Adequate care should also be

taken by the branch functionaries to seek only such information from the customer as is relevant to the risk category and is not intrusive.

The Company has adopted the following classification for risk categorization of its customers.

5.4.2 Definition of Customer Risk

'Customer Risk' in the present context refers to the money laundering risk associated with a particular customer from the Company's perspective.

5.4.2.1 High-Risk Customers (Category C)

Characteristics of High-Risk Customers: Customers whose source of funds is unclear or unconvincing shall be categorized as High-Risk customers. Enhanced due diligence shall be applied to this category of customers.

Indicative List:

- Multi-level marketing firms.
- Customers reported to FIU-IND under Suspicious Transaction Reporting (STR) or Cash Transaction Reporting (CTR) as per PMLA norms.

5.4.2.2 Medium-Risk Customers (Category B)

Characteristics of Medium-Risk Customers: Customers who are likely to pose a higher-than-average risk to the Company may be categorized as Medium-Risk customers.

Indicative List:

- Trusts/Societies that do not maintain books of accounts, other than Educational Trusts/Societies, charities, NGOs, and organizations receiving donations.
- Politically Exposed Persons (PEPs) as per RBI guidelines.

5.4.2.3 Low-Risk Customers (Category A)

Characteristics of Low-Risk Customers: Individuals and entities whose identities and sources of wealth can be easily identified, and whose account transactions largely conform to their known profile, shall fall under this category. Customers not covered under the High-Risk or Medium-Risk category definitions shall be categorized as Low-Risk customers.

Indicative List:

- Profiles engaged in transportation and related activities.
- Salaried employees, pensioners, and self-employed profiles.
- All entities with income documents such as Balance Sheets, Profit & Loss Statements, Bank Statements, and other documents from which the source of income/capital can be easily ascertained.

• Profiles that are not specified under the High-Risk or Medium-Risk categories.

5.4.2.4 Unacceptable Customers

Customers likely to pose the highest risk to the Company may be categorized as Unacceptable Customers, such as:

• Matches against terrorist lists, RBI watchlists, and country lists (indicative lists provided by IBA and the United Nations) during the de-duplication check.

• Private finance companies that are not registered with the RBI.

5.4.2.5 Existing Customers

• In the event of any change in risk profiling, the latest risk profile shall prevail.

• Customers reported to FIU-IND under Suspicious Transaction Reporting (STR) or Cash Transaction Reporting (CTR) as per PMLA norms shall be classified as High-Risk customers if their earlier classification was different.

5.4.2.6 Updation of Negative Database

The Company, through its Compliance, Business Intelligence & Analytics (BIA), and IT Departments, shall ensure that the de-duplication database is updated at specified intervals from the negative data sources mentioned below:

Terrorist Lists 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”, which includes the names of individuals and entities associated with Al-Qaida.

ii. The updated ISIL (Da'esh) & Al-Qaida Sanctions List is available at the prescribed UNSC website.

iii. The “1988 Sanctions List”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.

iv. In addition to the above, other UN sanctions circulated by the Reserve Bank of India and communicated by the Compliance Department in respect of other jurisdictions/entities from time to time shall be updated by the BIA and IT Departments for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

5.4.3 ONGOING DUE DILIGENCE

The Company shall undertake ongoing due diligence of customers to ensure that their transactions are consistent with the Company's knowledge of the customers, their business, risk profile, and source of funds. The extent of monitoring shall be aligned with the customer's risk category. The Risk Department shall review the indicative list for each risk category once every six months.

The Operations and Sales Departments shall periodically update customer identification data after the account is opened. The periodicity (from the date of account opening/last verification of KYC) of such updation shall not be less than once every ten years for Low-Risk customers, once every eight years for Medium-Risk customers, and once every two years for High-Risk customers, subject to the following conditions:

(a) Fresh proofs of identity and address shall not be sought at the time of periodic updation from customers categorized as 'Low Risk' where there is no change in their identity or address, and a self-certification to that effect is obtained.

(b) A certified copy of proof of address submitted by Low-Risk customers through mail/post, etc., in case of a change in address, shall be acceptable.

(c) Physical presence of the customer at the time of periodic updation shall not be insisted upon. Documents for the purpose of re-updation may be accepted through mail/post/courier, etc.

(d) The time limits prescribed above shall apply from the date of account opening/last verification of KYC.

(e) Fresh photographs shall be obtained from customers whose accounts were opened when they were minors, upon their attaining majority.

5.4.4 Policy on Risk-Based Approach for Periodic Updation of KYC Documents

The following risk-based approach for periodic updation of KYC has been adopted:

Periodic updation shall be carried out at least once every two years for High-Risk customers, once every eight years for Medium-Risk customers, and once every ten years for Low-Risk customers from the date of account opening/last KYC updation.

The Company may use Aadhaar OTP-based e-KYC in non-face-to-face mode for updation/periodic updation of KYC.

Low-Risk individual customers shall continue to be allowed transactions, and KYC updation may be completed within one year of becoming due or up to June 30, 2026, whichever is later.

The Company shall provide advance intimation and periodic reminders to customers for periodic updation of KYC through appropriate physical and/or digital communication channels in accordance with RBI guidelines issued from time to time.

1. Individual Customers

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

b) Change in address: In case there is a change only in the address details of the customer, a self-declaration of the new address shall be obtained through the customer's registered email

ID, registered mobile number, 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 letters, contact point verification, deliveries, etc.

2. Customers Other Than Individuals

a) No change in KYC information: In case there is no change in the KYC information of the legal entity customer, a self-declaration shall be obtained through the registered email ID of the legal entity, digital channels (such as online banking/internet banking/mobile application of the Company), a letter from an authorized official of the legal entity, Board Resolution, etc. Further, the Company shall ensure during this process that the Beneficial Ownership (BO) information available with it is accurate and updated wherever required.

b) Change in KYC information: In case of any change in KYC information, the RE shall undertake the KYC process equivalent to that applicable for onboarding a new legal entity customer.

3. Additional Measures

In addition to the above, the Company shall ensure that:

a) KYC documents of the customer as per the current CDD standards are available. This requirement applies even where there is no change in customer information but the documents available with the Company are not as per current CDD standards. Further, where the validity of the CDD documents available with the RE has expired at the time of periodic updation, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new customer.

b) The customer's PAN details, wherever available, are verified from the database of the issuing authority at the time of periodic updation of KYC.

c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant documents, including self-declarations, for carrying out periodic updation. Further, it shall be ensured that the information/documents obtained are promptly updated in the Company's records/database, and an intimation specifying the date of KYC updation is provided to the customer.

d) To ensure customer convenience, the Company may consider making available the facility for periodic updation of KYC at any branch.

e) The Company shall ensure that its internal KYC policy and processes relating to updation/periodic updation of KYC are transparent and that adverse actions against customers are avoided unless warranted by specific regulatory requirements.

5.5 AML PROCESS: TRANSACTION MONITORING

Ongoing monitoring is an essential element of effective KYC procedures. Effective control and mitigation of risks are possible only if there is a clear understanding of the normal and

reasonable activity of the customer. This, in turn, enables ACIPL to identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity of the account.

5.5.1 Types of Transactions to be Monitored

The following types of transactions should be closely monitored:

1. All cash transactions of a value exceeding Rupees Ten Lakh or its equivalent in foreign currency.
2. All series of cash transactions integrally connected to each other that have been individually valued below Rupees Ten Lakh or its equivalent in foreign currency, where such transactions have occurred within a month and the monthly aggregate exceeds Rupees Ten Lakh or its equivalent in foreign currency.
3. All cash transactions where forged or counterfeit currency notes or banknotes have been used as genuine and where any forgery of a valuable security has taken place.
4. All suspicious transactions, whether or not conducted in cash, and in the manner prescribed under the Rules framed by the Government of India under the Prevention of Money Laundering Act, 2002.

5.5.2 Instructions on Accepting Cash

i) It shall be ensured by every business unit that no cash of Rs. 50,000/- or above is accepted from a customer without obtaining a copy of the PAN Card. If the customer does not possess a PAN Card, a duly completed and signed Form 60 shall be obtained from the customer.

5.5.3 Information to be Preserved

Following information in respect of the above transactions has to be preserved:

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

5.5.4 REPORTING OF TRANSACTIONS

The PMLA and the Rules framed thereunder have imposed an obligation on the Principal Officer to report all cash transactions and suspicious transactions to the Financial Intelligence Unit (FIU-IND). There shall be no restrictions on operations in the accounts where an STR has been made. It should be ensured that there is no tipping-off to the customer at any level.

The types of transactions to be reported and the manner of reporting shall be as detailed below:

I. Reporting of Cash Transactions

The following types of transactions shall be reported to the FIU-IND:

i) All cash transactions of Rs. 10 lakh and above or its equivalent in foreign currency;

ii) 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 Rupees Ten Lakh or its equivalent in foreign currency.

Illustration of Integrally Connected Cash Transactions

The following transactions have taken place in an NBFC during the month of April 2008:

Date	**Mode**	**Dr. (in Rs.)**	**Cr. (in Rs.)**	**Balance (in Rs.)**
BF	-	-	-	8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly Summation		10,10,000.00	6,00,000.00	

1. As per the above clarification, the debit transactions in the above example are integrally connected cash transactions because the total cash debits during the calendar month exceed Rs. 10 lakh. However, ACIPL should report only the debit transactions that took place on 02/04/2008 and 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the NBFC, as it is less than Rs. 50,000.
2. All the credit transactions in the above example would not be treated as integrally connected, as the total of the credit transactions during the month does not exceed Rs. 10 lakh. Hence, the credit transactions dated 02/04/2008, 07/04/2008, and 08/04/2008 should not be reported.

Time of Reporting

i) The reporting of Cash Transactions to the FIU-IND shall be made only through the Principal Officer/Company Secretary appointed by the Company.

ii) Upon receipt of the documents referred to above, the Principal Officer and the Company Secretary shall report the Cash Transaction(s) referred to above to the Director, FIU-IND immediately, but not later than the 15th day of the succeeding month to which the transaction relates. While doing so, individual transactions below Rupees Fifty Thousand may not be included.

iii) This reporting shall be done in the prescribed format.

iv) Utmost confidentiality should be maintained while filing CTRs with FIU-IND.

II. Reporting of Suspicious Transactions

A 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 have no economic rationale or bona fide purpose; or

d. Gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

Explanation: A transaction involving financing of activities relating to terrorism includes transactions involving funds suspected to be linked or related to, or to be used for, terrorism, terrorist acts, a terrorist, a terrorist organization, or those who finance or are attempting to finance terrorism.

Apart from reporting cash transactions of the above nature, the Principal Officer and the Company Secretary are also under an obligation to report all transactions of a suspicious nature to the Director, FIU-IND. STRs should be filed if there are grounds to believe that the transaction involves proceeds of crime, irrespective of the amount involved and/or the threshold limit envisaged for predicate offences in Part B of the Schedule to the PMLA, 2002.

While furnishing information to the Director, FIU-IND, the delay of each day in not reporting a transaction or in rectifying a misrepresented transaction beyond the prescribed time limit shall constitute a separate violation.

The Company shall not impose any restriction on operations in accounts where an STR has been filed. The Company shall keep the fact of furnishing an STR strictly confidential. It shall be ensured that there is no tipping-off to the customer at any level.

Robust software generating alerts when transactions are inconsistent with the customer's risk categorization and updated profile shall be put to use as part of effective identification and reporting of suspicious transactions.

Indicative List of Suspicious Activities

1. Transactions Involving Large Amounts of Cash

Company transactions that are dominated by unusually large amounts of cash rather than cheques, electronic payments, etc.

2. Transactions That Do Not Make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited without adequate justification.

3. Activities Not Consistent with the Customer's Business

Accounts with large volumes of credits where the nature of the business does not justify such credits.

4. Attempts to Avoid Reporting/Record-Keeping Requirements

- A customer who is reluctant to provide information needed for a mandatory report.
- Any individual or group that coerces, induces, or attempts to coerce or induce an ACIPL employee not to file any reports or other forms.
- An account where there are several cash transactions below a specified threshold level to avoid the filing of reports.

5. Unusual Activities

Funds coming from countries/centres known for money laundering.

6. Customers Who Provide Insufficient or Suspicious Information

a. A customer/company that is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.

b. A customer/company that is reluctant to reveal details about its activities or provide financial statements.

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

7. Certain Employees Arousing Suspicion

a. An employee whose lavish lifestyle cannot be supported by his or her salary.

b. Negligence of employees or wilful blindness that is reported repeatedly.

8. Examples of Suspicious Activities/Transactions to Be Monitored by Operating Staff

a. Large cash transactions.

b. Multiple accounts under the same name.

c. Placing funds in term deposits and using them as security for additional loans.

d. Sudden surges in activity levels.

e. The same funds being moved repeatedly among several accounts.

Please Note: This is not an exhaustive list and is merely indicative.

Time of Reporting

i) The reporting of Suspicious Transactions to the FIU-IND shall be made only by the Principal Officer/Company Secretary appointed by the Company.

ii) Upon receipt of the above-referred annexures, the Principal Officer/Company Secretary shall report the Suspicious Transaction(s) to the Director, FIU-IND within seven days of arriving at the conclusion that a suspicious transaction has taken place.

iii) This reporting shall be done in the format prescribed by FIU-IND.

iv) The Principal Officer shall record the reasons for treating any transaction or series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such reports shall be made available to the competent authorities upon request.

v) It should further be noted that Suspicious Transaction Reports shall also be filed if there are reasonable grounds to believe that the transaction involves proceeds of crime, irrespective of the amount involved and/or the threshold limit envisaged for predicate offences in Part B of the Schedule to the PMLA, 2002.

vi) Utmost confidentiality should be maintained while filing STRs with FIU-IND.

5.5.5 REPORTING OF FORGED OR COUNTERFEIT CURRENCY NOTES OR BANK NOTES

All cash transactions where forged or counterfeit Indian currency notes or bank notes have been used as genuine, and where any forgery of a valuable security has taken place, shall be reported to the Principal Officer/Company Secretary in the manner prescribed below.

Time of Reporting

i) The reporting of the above-referred transactions to the FIU-IND shall be made only through the Principal Officer/Company Secretary appointed by the Company.

ii) Upon receipt of the CCR, the Principal Officer/Company Secretary shall report the said transaction(s) to the Director, FIU-IND by the 15th day of the succeeding month of occurrence of such transaction in the prescribed Summary Counterfeit Currency Report (CCR) format. Delay in reporting such transactions shall be construed as non-compliance.

Record Keeping

Central Operations (COPS) shall be responsible for the record keeping and retention of all documents as per the PMLA, 2002 Rules.

Records of all transactions shall be maintained for a period of five years from the date of the transaction between the customer and ACIPL. The documents are to be preserved in hard copy or digitized form (as may be intimated), so as to enable reconstruction of individual transactions (including the type and currency of the transaction involved, if any) and provide evidence, where necessary, for prosecution of persons involved in criminal activity.

Records pertaining to the identification of the customer and his/her address (e.g., copies of documents such as passports, identity cards, driving licences, PAN cards, utility bills, etc.) obtained while opening the account and during the course of the business relationship shall be properly preserved as mentioned above for at least five years after the business relationship has ended.

The following types of transactions are to be recorded and reported in the manner provided under the Reporting section of this Policy:

i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

ii) All series of cash transactions (pertaining to one customer or linked account, i.e., code and Group Code in SAP/BANCs) integrally connected to each other, which have been valued below Rupees Ten Lakh or its equivalent in foreign currency, where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

iii) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, and where any forgery of a valuable security has taken place;

iv) All suspicious transactions, whether or not made in cash, and in the manner as mentioned in the Rules framed by the Government of India under the Prevention of Money Laundering Act, 2002.

5.5.6 – Policy on Money Laundering & Terrorist Financing Risk Assessment

In order to maintain a constant check on the risks posed by money laundering and terrorist financing, a Risk Assessment shall be conducted by the Internal Audit Department (IAD).

i) IAD shall carry out a 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess, and take effective measures to mitigate money laundering and terrorist financing risks relating to clients, countries or geographic areas, products, services, transactions, or delivery channels, etc.

ii) The assessment process should consider all relevant risk factors before determining the overall level of risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of any overall sector-specific vulnerabilities that the regulator/supervisor may share with the Company from time to time.

iii) The risk assessment conducted by the Company shall be properly documented and 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 shall be reviewed at least annually.

iv) The outcome of the assessment shall be placed before the Board or any committee of the Board to which powers in this regard have been delegated and shall be made available to competent authorities and self-regulating bodies.

v) The suggestions and mitigants approved by the Board shall be implemented. IAD shall monitor the implementation of the controls and enhance them, if necessary. The Company shall apply a Risk-Based Approach (RBA) for the mitigation and management of identified risks and shall have Board-approved policies, controls, and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them, if necessary.

vi) IAD shall decide suitable processes/procedural aspects through the Chief Internal Auditor, based on the above guidelines, for implementation of the same.

5.6 BUSINESS PARTNER DUE DILIGENCE PROCEDURE

5.6.1 BUSINESS PARTNER DUE DILIGENCE (BPDD)

Definition

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

The Outsourcing Policy of ACIPL governs all Business Partner relationships.

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

- Empaneled Lawyers
- Empaneled Valuers
- Vendors providing services such as Selling Agents, Direct Selling Teams/Agents, Collection Agencies, Verification Agencies, Bidders, etc.
- Any other intermediary.

ACIPL shall collect all KYC documents as specified in the Annexures.

Due Diligence of Business Partners

Business Partner relationships are entered into at the Corporate Office/Regional Office/Head Office level. Hence, the Heads of Business Units/Departments are responsible for ensuring that adequate due diligence measures are applied before accepting a Business Partner.

The following procedure shall be followed:

Step 1

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

(i) The Business Partner as defined above.

(ii) Individuals who are authorized to act on behalf of the Business Partner.

(iii) The Beneficial Owner (BO) of the Business Partner.

Step 2

The Heads of Business Units/Departments should screen the names and dates of birth/other relevant data of the Business Partner and its BOs/Representatives against the freeze lists/negative lists/Dedup database.

In case of a hit against any of the screened lists, enhanced measures should be applied to ascertain the identity of the Business Partner. The enhanced measures shall be the same as those applicable under Customer Acceptance procedures.

Step 3

A pre-employment screening of the staff of the Business Partners who have or may have access to ACIPL's data or systems should be performed.

Review of Business Partners

Periodicity

The Business Partner files shall be reviewed whenever any material change comes to the notice of ACIPL. Records of Business Partners should be reviewed annually by the Sales and Operations Departments.

Step 1

The Business Unit/Department that has performed the due diligence while onboarding the Business Partner shall also be responsible for the periodic review. The Audit Department shall monitor and ensure that all Business Units/Departments comply with this procedure and perform timely reviews.

Step 2

The review shall be performed using the Due Diligence Form for Business Partners. The revised Due Diligence Forms should be maintained along with the Agreement.

5.7 ANNEXURES

ANNEXURE A1 - DOCUMENTATION

Officially Valid Document (OVD): OVD means one of the following documents with OSV (physical/digital/electronic):

1. Valid Passport issued in India.
2. Valid Permanent Driving License (unexpired).
3. Aadhaar Card* (letter issued by the Unique Identification Authority of India containing details of name, address, and Aadhaar number).
4. Voter Identity Card issued by the Election Commission of India.
5. Valid Job Card issued under NREGA, duly signed by an officer of the State Government.
6. Letter issued by the National Population Register containing details of name and address.

* Aadhaar Number Validation & Redaction – Company shall, where its customer consents to submit his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means. RBI has allowed for Offline verification in such cases.

Important points

- Where Permanent Account Number (PAN) is obtained, the same shall be verified from verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- Copies of the KYC documents (physical / digital) should be verified with originals and certified by the person verifying the same as 'True Copy' i.e. Original, Seen and Verified (OSV). The ACIPL Employee or ACIPL Representative who meets the customer should perform the verification (OSV stamp with name, signature and employee / representative code) in physical/digital/electronic mode.
- The KYC documents scanned/uploaded in digital/electronic mode shall be stored in system and it should be available for reference as and when required. In such cases, physical copy may not be stored.
- KYC documents of Beneficial Owner (BO) has to be mandatorily collected. BO is defined as per Annexure A2.

- KYC documents issued in incomplete names (only personal names (first names) as in the case of Voter ID in certain states) cannot be accepted.
- KYC documents collected for address proof should contain the complete address as captured in the application form. If there is any difference or if the details are incomplete (as per manual check or rule engine based system check), then another document containing the address as per application form should be taken.
- Marriage Certificate issued by state govt. or gazette notification to be used in case of name change along with certified copy of KYC documents in existing name to be obtained for identity and address proof of the person and can be used for relationship proof.
- In case of a partnership between individual(s) and entity(s) or between entity(s), the KYC requirements for such entity(s) also need to be complied with in addition to the KYC requirements of the partnership.
- KYC document/information can be validated digitally through external vendors appointed by the company. Any of the following i.e. Physical or manual mode / Optical Character Recognition (OCR) / Digital Scanning can be used to capture the information. Information captured though OCR / Scanning and the information validated through external vendor should match as per the logics specified in system based rule engine.
- In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained: Authorised officials of overseas branches of Scheduled Commercial Banks registered in India, Branches of overseas banks with whom Indian banks have relationships, Notary Public abroad, Court Magistrate, Judge, or Indian Embassy/Consulate General in the country where the non-resident customer resides.
- Where OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

KYC DOCUMENTATION

Customer Type	Documents Required
Individual	The Company shall obtain the following from an individual (applicant, co-applicant, guarantor) while establishing an account-based relationship or while dealing with an individual who is a Beneficial Owner, authorised signatory, or power of attorney holder related to any legal entity or customer/transaction as defined in the 'Applicability Section': 1. Recent colour passport-size photograph (physical/digital/selfie) 2. Permanent Account Number issued by Income Tax Authority (mandatory) 3. Aadhaar Card (letter issued by the Unique Identification Authority of India containing details of name, address, and Aadhaar number). Aadhaar may be taken with offline verification of a customer if he is desirous of undergoing the same and the

	address in Aadhaar is updated (i.e., same as per application form where customer is residing currently). Alternatively, any one of the other valid OVDs with updated address shall be taken. If still the OVD furnished by the customer does not have the updated address, then any of the following additional documents with updated address shall be taken for the purpose of proof of address: (a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) Property or municipal tax receipt; (c) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (d) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation. Where the Permanent Account Number is not available, the individual applicant shall submit Form 60; also, one of the OVDs as mentioned above would be required for identity proof.
Proprietorship	• Documents in the name of proprietor (Individual) as mentioned in the "Individual" section for details of identity and address of the individual (proprietor); and • In addition to the above, any two of the following documents as proof of business/activity in the name of the proprietary firm shall also be obtained: (a) Registration certificate (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act (c) Sales and income tax returns (d) CST/VAT/GST certificate (provisional/final) (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities (f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities (h) Utility bills such as electricity, water, landline telephone bills, etc.

	In cases where ACIPL is satisfied that it is not possible to furnish two such documents, then one of the above documents can be accepted, subject to contact point verification by ACIPL employee/BDM or CPV is done by CPV agencies to collect all such information as would be required to establish the existence of such firm, confirm, clarify, and satisfy themselves that the business activity has been verified from the address of the proprietorship firm. In instances where CPV is not done by ACIPL employee, tele-verification by ACIPL employee needs to be mandatorily documented in the file.
Registered Partnership Firm	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Registration certificate 2. Copy of Partnership Deed (partnership deed should contain a provision for borrowing clause covering hypothecation/creating charge on the asset belonging to the firm and giving guarantee) executed on stamp paper or franked and signed by all partners at least on last page under authority stamp (for capacity) 3. Partnership Authority Letter (PAL): All pages of the Partnership Letter to be signed by minimum one partner. All partners should sign and authenticate at least the last page of the PAL under rubber seal (for capacity). The PAL should be on the firm's letterhead. Any alterations on any page to be signed by all the partners. 4. Copy of PAN Card in the name of partnership firm 5. Documents as specified in Individual section for the partner, BO, authorised signatories, and individual holding an attorney to transact on firm’s behalf.
Public/Private Limited Company	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Board Resolution to apply and avail the loan and power of attorney granted to its managers, officers or employees to transact on its behalf 2. Certified true copy of Board Resolution from the Company Secretary/Managing Director to the effect that the person signing the loan document has the authority to execute the deal on behalf of the company along with the extract of the Board Resolution in this respect 3. Latest list of all directors with their addresses signed and dated by the Company Secretary/Directors so as to ensure the certifying director’s name is in the list of directors submitted by the company. Refer Annexure A4 in case of change of directorship 4. Copy of PAN Card in the name of company 5. Copy of Certificate of Incorporation (COI), Memorandum of Association (MOA), Articles of Association (AOA) verified with original. Copy of certificate of commencement of business in case of public limited companies. The AOA should permit the company to borrow and give a guarantee 6. Documents as applicable for individuals, authorised signatories, and BO as specified in “Individuals” section

	7. Certified information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding
Trust/Association/Society/Club/University (Registered)	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Registration certificate 2. Copy of PAN in the name of entity 3. Certified "true and updated" copy of Trust Deed/Bye-laws/MOA attested by Secretary/Managing Trustee/Chairperson 4. Certified "true and updated" copy of certificate of registration (for club/society/association/trust) signed by the secretary 5. List of all office bearers/trustees along with settlers (including any person settling assets into the trust), grantors, protectors, beneficiaries (when they are defined) and, in case of foundations, founders/managers/directors, to be obtained on letterhead with their addresses 6. Certified copy of resolution to borrow facility/loan signed by managing trustee/chairperson/secretary 7. Documents of trustee, BO and authorised signatory signing the facility/loan documents as specified in "Individuals" section above 8. Notarised power of attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract on behalf of the firm. Certified copy of OVD of POA holder has to be obtained. Notarised POA would not be required if one or more members of the trust/society/etc. are directly executing the contract. (Annexure A5) 9. Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding.
Hindu Undivided Family (HUF)	One certified copy of each of the following documents shall be obtained: 1. HUF letter with specimen signatures of the Karta and all adult co-parceners as per HUF declaration format provided in Annexure A3 2. PAN Card in the name of HUF 3. Documents of Karta (as applicable for Individuals) 4. Address proof of the HUF: (a) Latest available Income Assessment Order OR (b) Bank statement of account with existing banker (scheduled bank) bearing the account holder's address with entries of preceding 3 calendar months from the date of login
Unregistered Association/Body of Individuals / Trusts / Partnership Firms / Universities / Local Bodies	One certified copy of each of the following documents or equivalent e-documents shall be obtained: 1. Resolution of the managing body of such association or body of individuals (PAL will be applicable for partnership firm) 2. Copy of PAN in the name of entity 3. Certified "true and updated" copy of Trust Deed/Bye-laws/MOA attested by Secretary/Managing Trustee/Chairperson 4. Partnership Authority Letter (PAL): All pages of the Partnership Letter to be signed by minimum one partner. All

	partners should sign and authenticate at least the last page of the PAL under rubber seal (for capacity). The PAL should be on the firm's letterhead. Any alterations on any page to be signed by all partners. Certified copy of OVD in respect of the person holding a PAL to transact on its behalf 5. Notarised power of attorney granted to managers, officers or employees of the firm to transact business on its behalf, if such managers, officers or employees are entering into the contract on behalf of the firm. Certified copy of OVD of POA holder has to be obtained. Notarised POA would not be required if one or more partners of the firm are directly executing the contract (Annexure B4). 6. Proof of legal existence of such entity in the form of Service Tax/VAT/Sales Tax Registration/CST/VAT/GST certificate/certificate of registration document issued by Sales Tax/Service Tax/Professional Tax authorities/Udyog Aadhaar Registration Certificate. 7. Information to be collected about the shareholding/ownership share/profit share/beneficiary for establishing percentage holding. Explanation: Term 'body of individuals' includes societies

ANNEXURE A2

PROCESS OF DETERMINATION OF BO:

1. Where the client is a person other than an individual or trust:

   A. BO is the person exercising control through ownership interest. Where the non-individual client is:

   i. Company:

   1. A person having ownership of/entitlement to more than 10 percent of shares or capital or profits of the said company, or

   2. A person having 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, shall be the BO of the company.

   ii. Partnership Firm: A person having ownership of/entitlement to more than 10% of the capital or profits of the partnership firm shall be the BO.

   iii. Unincorporated association or body of individuals: A person having ownership of/entitlement to more than 15% of the property or capital or profits of the unincorporated association or body of individuals shall be the BO.

   B. Where no natural person exerts control through ownership interests, BO shall be the person exercising control over the non-individual client through other means like control over voting rights, agreements, arrangements, etc.

   C. Where no natural person is identified under (a) or (b) above, BO shall be the person who holds the position of senior managing official of the non-individual client.

2. Where the client is a trust: BO shall be:

   A. Author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust.

   B. Any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3. Where the client or the owner of the controlling interest is a company listed on a stock exchange or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or Beneficial Owner of such companies.

ANNEXURE A3

HINDU UNDIVIDED FAMILY LETTER

Date:

To,

Abhiyan Capital (India) Pvt. Ltd.

Branch.

Dear Sir,

The business of …… carried on in the firm name and style of …… at …… is the ancestral business of the Joint Hindu Family governed by the Mitakshara/Dayabhaga Law, of which I/we, the undersigned, am/are the present Karta or Managing Member(s), and we, the undersigned, are the present adult members. As the aforesaid joint family business, by its nature, cannot be carried on without credit facilities, we have requested you to finance the aforesaid joint family business of the firm and to grant to the firm all or some or any of the credit facilities that may be agreed upon from time to time between you and the Joint Hindu Family firm for sums not exceeding at any one time in the aggregate sum of Rs. _____ (Rupees _____ only).

The following members, viz.:

1. ……
2. ……

are authorized jointly or severally to represent and sign on behalf of the said joint family business in the manner as appears below and have full and unrestricted authority to bind all the members of the joint family, however constituted from time to time.

In the event of you acceding to our request and granting us the facility applied for financing, we, the undersigned, undertake with the intention of binding not only the present members of the said joint family (both adults and minors) but also all future members thereof (both adults and minors) and all persons entitled to a share therein, and ourselves personally and our respective interests in the joint family properties as well as our separate estates.

1. Whenever any change occurs in the managership or in the nature of the said ancestral business or in the constitution of the said joint family or said ancestral business, caused by the death of a co-parcener whether or not resulting in the share devolving on his widow or widows, or by the birth of a co-parcener, or if at any time any of us desire to give up or sever his connection with the said ancestral business, or if we desire to close the said ancestral business, or if any minor member of the said family attains majority, we shall give notice thereof to you at once in writing; and

2. Until receipt of such notice by you, and whether or not any provisions of the Partnership Act, 1932 shall apply, you shall be entitled to regard each of us as partners in respect of all dealings or transactions with you which may be found to be outside the scope of the said ancestral business, and such dealings and transactions shall be binding on each of us as such partner and our respective estates; and

3. Notwithstanding any provisions of the said Act or any change in the membership of the said firm, all acts purporting to be done on behalf of the said joint family business before you have received notice in the manner aforesaid shall be binding on the said joint family and its properties and on each of us and our respective estates, and the liability of the said firm and of each of us and of our respective estates shall continue until all liabilities in respect of such acts shall have been discharged.

The names and dates of birth of the present minor members of the aforesaid joint family are given below:

Yours faithfully,

(Signature)

1. Shri ……. His personal signature here

   Will sign on behalf of the firm as follows: Karta

2. Shri ……. His personal signature here

   Will sign on behalf of the firm as follows:

**Particulars of the minor members of the joint family*

Name | Father's Name | Date of Birth

ANNEXURE A4

DECLARATION CUM INDEMNITY (Confirming List of Directors)

To,
Abhiyan Capital (India) Limited
(Branch Address)

Kind Attn: _____

Dear Sir,
_____, a company registered under _____ and having its registered office at _____ (complete office address) (hereinafter referred to as "the Company"), do hereby declare and state as under:

As on the date of this Declaration cum Indemnity, the following are the directors of the Company:

The Company hereby confirms that all the requisite legal formalities for appointment of the above-mentioned directors have been complied with, including filing of Form 32 with the Office of the Registrar of Companies.

The Company hereby confirms that it has applied to ACIPL for obtaining a _____ (type of loan/facility) at the _____ (branch), and that the Company has to submit various documents to ACIPL with respect to the application for the said account. The Company further states that it is unable to furnish to ACIPL a copy of Form 32 filed with the Office of the Registrar of Companies with respect to the appointment of Mr. _____ as a director on account of the same having been misplaced / due to change in directors since incorporation.

The Company hereby agrees and undertakes to hold harmless and keep ACIPL fully indemnified against any claims and damages which may be made in respect hereof by reason of ACIPL relying and acting upon the faith of this Declaration cum Indemnity.

The Company further agrees and undertakes to pay and make good all such losses, damages, or expenses upon demand, and also to comply with such requirements, including furnishing or executing such further deeds, documents, or writings as ACIPL may require.

Signed and delivered by _____ through its authorized signatory Mr. _____ in the presence of:

(Stamp and Seal of Company)
Place: _____
Date: _____

ANNEXURE A5
FORMAT FOR POWER OF ATTORNEY
(Stamp Duty as per State Laws and to be Notarized)

SPECIFIC POWER OF ATTORNEY

Be it known to all to whom it may concern that we, _____ s/o _____ aged about _____, residing at _____;
_____ s/o _____ aged about _____, residing at _____;
_____ s/o _____ aged about _____, residing at _____;
and _____ s/o _____ aged about _____, residing at _____, presently acting as Partners of the Partnership Firm M/s _____ bearing registration no. _____ (in case of registered Partnership Firm), having its place of business/address at _____, do hereby nominate, constitute, and appoint _____ s/o _____ aged about _____, presently a Partner, as our Attorney to do the following acts, deeds, and things on behalf of all of us jointly and severally in our name in respect of the Loan _____:

1. That we are the partners of the partnership firm, M/s _____.
2. That the partnership firm is considering availing a loan / giving guarantee for a loan of Rs. _____ from Abhiyan Capital (India) Limited (hereinafter to be known as "ACIPL") for the purpose of _____.
3. That we hereby jointly and severally appoint and authorize Mr. _____ s/o _____ aged about _____ years, who is presently a partner, to do all or any of the above acts, or any other acts which have not been specifically mentioned herein above, and which in the opinion of our attorney ought to be done, executed, or performed in respect of the said loan or any matter incidental thereto.
4. That all the acts done and documents executed by the aforesaid partner shall bind the firm and each of us as if each of us had ourselves done such acts and executed such documents.
5. That the acts, deeds, and things done or caused to be done by our attorney for the said purpose shall be construed as acts, deeds, and things done by the firm and all of us jointly and severally. All of us shall be jointly and severally responsible for the liabilities of the said firm, and ACIPL may recover its claims and dues from any or all of the partners of the firm and the estate of the deceased partners.
6. This Power of Attorney supersedes all previous Powers of Attorney or any other authorization in relation to this loan.

IN WITNESS WHEREOF, we the executants have put our hands on these presents on the date, month, and year herein below mentioned in the presence of the following witnesses:

Signature of the Partner: _____
Name of the Partner: _____
Signature of the Partner: _____
Name of the Partner: _____
Signature of the Partner: _____
Name of the Partner: _____
Signature of the Partner: _____
Name of the Partner: _____
Place: _____
Date: __ / __ / 20XX
Witness: _____

Additional Governance & Compliance Enhancements
All references to ACIPL / Abhiyan Capital (India) shall be updated to the current legal entity name of the Company across policy, annexures, forms, and SOPs. Any exceptional KYC measures, enhanced due diligence norms, or risk-based deviations shall form part of the Board-approved KYC Policy.

Additional RBI Compliance Enhancements – Final Updates
Reporting to RBI: The name, designation, address, and contact details of the Principal Officer and Designated Director shall also be communicated to the Reserve Bank of India in addition to FIU-IND.

Group-wide AML/CFT/PF Programme: The Company shall implement group-wide AML/CFT/PF policies and procedures, including sharing of customer, transaction, and risk information within group entities, subject to confidentiality safeguards and prevention of tipping-off.

CKYCR Compliance: The Company shall upload KYC records to CKYCR within prescribed timelines and retrieve customer KYC records using the KYC Identifier wherever applicable. Where a valid CKYCR record exists, fresh collection of KYC records shall not be insisted upon except where additional documents are required under a risk-based approach.

Periodic KYC Intimation: The Company shall provide advance intimations and reminders to customers regarding periodic updation of KYC as prescribed by RBI from time to time, including at least one communication through physical letter/email/SMS/other digital modes before and after the due date.

Customer Obligation for Change in KYC: Customers shall submit updated OVDs/documents within 30 days of any change in KYC information, including address, contact details, beneficial ownership, or constitution.

Beneficial Ownership Threshold: Beneficial ownership identification shall be carried out in accordance with RBI Master Direction – KYC, including: Company – more than 10%; Partnership – more than 10%; Unincorporated Association – more than 15%; Trust Beneficiary – 10% or more beneficial interest.

V-CIP Cloud/Data Requirement: Where cloud infrastructure or third-party service providers are used for V-CIP, ownership of customer data, videos, and audit trail shall remain with the Company, and no data shall be retained, stored, or processed by service providers beyond regulatory and contractual permissions.

****End of Know Your Customers (KYC) and Prevention of Money Laundering (PML) Policy****