ANTI-MONEY LAUNDERING (AML)/ KNOW YOUR CUSTOMER (KYC)/ COMBATING FINANCING OF TERRORISM (CFT) POLICY

INDEX

1. INTRODUCTION

CNH Industrial Capital (India) Private Limited ("CNH Capital" or "the Company"), by means of this Policy, aims to adopt and implement Know Your Customer (KYC), Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT) standards in its day-to-day practice. These standards are applied when working with our dealers as well as our agricultural and construction customers.

The Board of Directors has formulated this Policy in line with the Prevention of Money Laundering Act (PMLA), 2002 and related amendments; Prevention of Money Laundering (PML) Rules, 2005 and related amendments; RBI KYC – Master Directions, 2016; Centralised KYC Registry (CKYC) Guidelines; and Master Directions for Non – Banking Financial Company (Systemically important Non- Deposit taking Company), 2016.

The Board of Directors has the ultimate responsibility for adoption and implementation of the KYC/AML/CFT framework.

2. OBJECTIVE OF THE POLICY

The objective of this policy is for CNH Capital to know / understand its customers and their businesses thereby allowing the Company to manage its AML risks prudently. It also prevents the Company from being used, intentionally or unintentionally, by criminal elements for money laundering and other illicit activities. CNH Capital endeavours to ensure compliance and adoption of KYC/AML/CFT regulations by all its directors, employees, and agents, by means of this policy.

3. KEY DEFINITIONS

3.1 For the purpose of this policy and related process documents, key terms have been defined as follows:

i. "**Aadhaar number**" means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.;

ii. "**Central KYC Records Registry**" (CKYCR) means an entity defined under Rule 2(1) (aa) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (the "Rules"), to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

iii. "**Designated Director**" means a person designated as Managing Director or a whole-time Director duly authorised by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering (PML) Act and the Rules.

iv. **"Digital KYC"** has been defined in Section 3 as capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Reporting Entity (RE) as per the provisions contained in the Act. Steps to carry out the Digital KYC process have also been stipulated in Annex - I.

v. **"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.

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

vii. "**Officially valid document"** (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by Mahatma Gandhi National Rural Employment Guarantee Act (NREGA) duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and address.

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

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

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

ii. property or Municipal tax receipt;

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

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

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

d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

viii. **"Principal Officer"** means an officer nominated by the Company who is responsible for furnishing information, implementation of this policy, making various reporting and liaising with the RBI.

ix. **"Suspicious transaction"** means a "transaction" 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 in the Schedule to the PMLA, regardless of the value involved; or

b) appears to be made in circumstances of unusual or unjustified complexity; or

c) appears to not have economic rationale or bona-fide purpose; or

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

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

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

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

xi. Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction. Details procedure explained in **Appendix 3.**

xii. "**Customer/client"** means a person who is engaged in a financial transaction or activity with CNH Capital and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

xiii. "**Customer Due Diligence"** (CDD) means identifying and verifying the customer and the beneficial owner based on information and documents as mentioned in the Appendix 2, including following the e-KYC process.

xiv. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

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

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

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

xviii. "**Beneficial Owner"** shall mean person(s) as explained in **Appendix 1.**

4. SCOPE OF THE POLICY

4.1 Customer Acceptance Policy

The Company's Customer Acceptance Policy articulates the criteria for the acceptance of customers.

4.1.1. Customer Acceptance Policy (CAP)

The following principles shall be adhered to at the time of customer acceptance:

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

ii. Accept customers only after verifying their identity, as mentioned under this Policy.

iii. Not to open a loan account or commence a financial relationship where the identity of the customer cannot be verified and/or documents/information required could not be obtained / confirmed due to non-cooperation or non-reliability of the customer.

iv. No transaction or account based relationship is undertaken without following the CDD procedure.

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

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

vii. Identity of a new customer to be checked to ensure that it does not match with any person with a known criminal background.

viii. Documentation requirements and other information to be collected for KYC are to be complied with.

ix. Loan accounts of persons having relationships with banned persons / entities such as individual terrorists or terrorist organizations etc. are not to be opened. Further, loan accounts should not be opened for persons convicted of nefarious activities such as money laundering, terrorism, drug trafficking, bank fraud etc.

x. No loan account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India or United Nations or explicitly prohibited by the RBI.

xi. No loan account shall be opened if the Company is of the opinion that the customer may expose the Company to KYC/AML/CFT risks.

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

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

4.2 Adoption of Risk based approach

CNH Capital customers will be categorized based on factors such as nature of the loan product availed, customer background and business (social and economic standing), amount involved, location etc. , into three categories – low risk, medium risk and high risk. No customer will be exempted from the Company's.

KYC procedure, irrespective of the status and relationship with the Company or CNH Industrial Group. The above requirement may be moderated according to the risk perception.

4.2.1 High Risk : High risk customers typically include:

(a) firms with sleeping partners;

(b) politically exposed persons (PEPs);

(c) individuals with dubious reputation as per public information available in consideration with the Customer Acceptance Policy.

(d) trust, charitable organizations, non-government organizations (NGO)

(e) high net worth individuals (e.g. net worth exceeding INR 200 lakhs)

4.2.2 Medium Risk : Medium risk customers will typically include:

(a) non-resident customers

4.2.3 Low Risk : Low risk customers will typically include:

(a) individuals and entities whose identities and sources of wealth can be easily identified.

(b) entities such as commercial banks and financial institutions that are registered with statutory bodies like Reserve Bank of India, Government companies or any organization owned or controlled by the Indian Government may also be categorised as low risk.

The Company shall obtain the required data/documents, other relevant information, and credit risk profiles of the customers and apply various Anti Money Laundering measures keeping in view the risk involved in a transaction and perform enhanced due diligence, for medium and high risk customers.

4.3 Customer Identification Procedure (CIP):

4.3.1 Customer Identification Procedure means undertaking client due diligence measures while commencing a financing-based relationship including identifying and verifying the customer and the beneficial owner based on information and documents as mentioned in the Appendix 2, including following the e-KYC process.

4.3.2 CNH Capital shall undertake identification of customers in the following cases:

(a) Commencement of a new relationship with the customer.

(b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(c) When there are suspicions of money laundering or financing of activities relating to terrorism, for existing customers.

(d) When carrying out any transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(e) When 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.

(f) 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.

4.3.3 For the purpose of verifying the identity of customers at the time of commencement of a new relationship, the Company will at its option, rely on customer due diligence done by a third-party, subject to the following conditions:

(a) The required information of such customers' due diligence, carried out by the third-party, is obtained within two days from the third party or from the CKYCR by the Company.

(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 from the third-party upon request immediately.

(c) The third-party is regulated, supervised or monitored for, 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, will be with CNH Capital.

4.4 Customer Due Diligence (CDD)

While undertaking customer identification, the Company will ensure that decision making functions of determining compliance with KYC norms shall not be outsourced. CNH Capital shall apply customer due diligence measures to all clients based on the materiality and risk and conduct due diligence on relationships at appropriate times. CDD for KYC provided in **Appendix 2**.

4.4.1 Certain key checks will be undertaken for the purpose of customer due diligence:

- Checking customer details against the UN Sanctions list
- Check to determine if the customer is a PEP
- Check to determine the Ultimate Beneficial Owner (UBO)
- Check against internal blacklists
- Check whether Non-resident Indians (NRIs)/ Overseas Citizen of India (OCI) customers are operating in high risk jurisdictions/jurisdictions that do not or insufficiently apply the FATF recommendations
- Any other checks as may be required by the RBI and Government of India

Acceptance of PEP customers for the purpose of providing financing facilities shall be approved by the Designated Director.

4.4.2 CNH Capital Customer ID

While establishing a financing-based relationship, the Company to ascertain as to whether the customer is already having a Customer ID with the Company. In case the customer

has an existing Customer ID, fresh Customer ID shall not be created and the new account shall be opened with the existing Customer ID.

4.4.3 Identification of Beneficial Owner (BO)

Beneficial Owner , as has been defined in "**Appendix 1**" , for opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to verify their identity shall be undertaken.

4.4.4 On-going Due Diligence

A) CNH Capital will undertake on-going due diligence of customers to ensure that their transactions are consistent with its knowledge about the customers, customers' business and risk profile; and the source of funds.

B) Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

(a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
(c) High account turnover inconsistent with the size of the balance maintained.
(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

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

Explanation: High risk account have to be subjected to more intensified monitoring.

a. Review of risk categorization of customers will be conducted every six months and enhanced due diligence will be implemented accordingly for high risk customers.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

4.4.5 Periodic Updation

The Company shall adopt a risk-based approach for periodic updation of KYC. Periodic updation of all KYC information of the customers shall be carried out at least once every two-years for high risk customers, once every eight-years for medium risk customers and once in every ten years for low risk customers:

- The time limits prescribed above apply from the date of opening of the account or last verification of KYC / last KYC updation, whichever is more recent.

a) Individual Customers:

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

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

b) Customers other than individuals:

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

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

c) Additional measures: In addition to the above, the Company shall ensure that:

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

ii. Customer's PAN details, if available with the Company verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegatedthe Company.

4.4.6 Enhanced Due Diligence for specific clientele

(I) **Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):** The Company shall ensure that the first payment is to be effected through the customer's KYC-complied account with another Bank(s)/Financial Institution(s) for enhanced due diligence of non-face-to-face customers.

(II) Accounts of Politically Exposed Persons (PEPs)

A. CNH Capital will have the option of establishing a relationship with PEPs provided that:

(1) sufficient information including information about the sources of funds is gathered on the PEP;

(2) the identity of the person shall have been verified before accepting the PEP as a customer;

(3) the decision to provide financing to a PEP is taken by the "Designated Director" in accordance with the Company's Customer Acceptance Policy;

(4) the CDD measures as applicable to PEPs, including enhanced monitoring are applicable

(5) designated director approval for continuing the business relationship shall be sought in the event an existing client becomes a PEP.

(6) all such accounts are subjected to enhanced monitoring on an on-going basis are applicable

B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

4.5 Transaction Monitoring

4.5.1 The transaction monitoring will be based on the following principles:

a. The Company will seek to understand the background and expected transactional behavior of the customer, so that activities that do not complement such understanding can be detected.

b. Particular attention should be paid to the following types of transactions:

1. Down-payments, excluding trade-ins, greater than 40% purchase price;

2. Large transactions (i.e. four pre-payments or more on a retail account);

3. Refunds to retail customers greater than INR 0.5 lakhs;

4. Retail payouts within the first 45-days of financing;

5. Payment via third-party cheques, drafts, etc. on a retail customer or dealers account;

6. Unidentified customer remittances;

7. Unapplied cash and credit notes on a dealer statement in excess of INR 50 lakhs;

8. Transactions with unusual patterns, inconsistent with the normal and expected activity of the dealer and which may exceed thresholds specified for certain accounts.

c. Supervisors should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the borrowers. In case of any doubt, make necessary enquiries with the borrowers.

d. Threshold limits for specific customers/accounts may be prescribed and attention will be paid to transactions that exceed these limits

e. While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.

f. All the staff members are instructed to maintain the standards of good conduct and behaviour expected of them and not to involve in any activity that would bring disrepute to the Company and not to tip-off potential customers on processes which could undermine the KYC norms or the norms of due diligence prescribed by RBI from time to time.

4.6 Reporting to and Registrations with Financial Intelligence Unit – India (FIU-IND)

4.6.1 As per the requirement of PML Act, 2002, and the Rules there under, the following information shall be furnished to FIU-IND:

a. all cash transactions of the value of more than INR 10 lakhs or its equivalent in foreign currency;

a. all series of cash transactions integrally connected to each other which have been individually valued below INR 10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds and amount of INR 10 lakhs or its equivalent in foreign currency;

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

c. all suspicious transactions, as defined previously, whether or not made in cash

4.6.2 The Company shall formulate internal mechanism for detecting transactions as mentioned above and for furnishing information about such transactions as specified by FIU-IND and the RBI.

4.6.3 Various Reporting and Registrations

A. The Company shall undertake registration with FIU-IND.

B. Name, designation and address of the "Designated Director" and any subsequent changes shall be communicated to FIU-IND.

C. Name, designation and address of the "Principal Officer" and any subsequent changes shall be communicated to FIU-IND.

D. Cash Transaction Report (CTR)
Cash Transaction Report (CTR) with respect to transaction mentioned in Section 4.6.1 (a) and (b) above, for each month shall be submitted by the Principal Officer to FIU-IND by the 15th day of the succeeding month.

E. Counterfeit Currency Report (CCR)
A CCR, with respect to transactions mentioned in Section 4.6.1 (c) above, for each month shall be submitted by the Principal Officer to FIU-IND by 15th day of the succeeding month.

F. Suspicious Transaction Reports (STR)
An STR, with respect to transactions mentioned in Section 4.6.1 (d) above, shall be submitted by the Principal Officer to FIU-IND promptly not later than seven working days on being satisfied that the transaction is suspicious.

The Principal Officer shall furnish all the reports mentioned above based on the information available with the Company. He shall retain a copy of such information for the purposes of official record. It shall be the responsibility of CNH Capital and its Designated Director, officers

and employees to follow the
manner and procedure of furnishing information as specified by FIU-IND/RBI.

There shall be no tipping off to the customers at any point of time.

Additionally, as per CFT norms, details of individuals/ entities that match UN Sanctions lists shall be immediately reported to FIU-IND and RBI.

4.7 Record Keeping

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. CNH Capital will,

(a) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;

(b) maintain all necessary records of transactions between the Company and the customer for at least five-years from the date of transaction. Necessary information in respect of transactions so as to permit reconstruction of individual transaction, shall also include the following:;

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

(c) preserve the records pertaining to the identification of the customers obtained while opening the account and during the course of business relationship, for at least five-years after the business relationship is ended;

(d) make available the identification records and transaction data to the competent authorities upon request;

(e) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(f) maintain records of the identity and address of its customer, and records in respect of transactions in hard or soft format.

It shall be the responsibility of CNH Capital and its Designated Director, officers and employees to observe the procedure and manner of maintaining information

4.8 Confidentiality of Information

Information collected from the customer for the purpose of applying for credit shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling etc. Information

sought from the customer shall
be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer shall be requested for with their express consent and

in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

4.9 Combating financing of terrorism (CFT)

The United Nations Security Council (UNSC) periodically circulates lists of individuals and entities, suspected of having terrorist links. The United Nations Security Council Resolutions (UNSCRs) shall be taken into account.

The Company is required:

- to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/or financing a customer.

- to ensure that the name(s) of the proposed customer does not match with that of the United Nations list of Terrorist individuals/organization/ entities, before financing a customer.

In order to ensure compliance with the CFT Norms prescribed, the Company will ensure compliance with:

- The Unlawful Activities (Prevention) Act, 1967 (UAPA), its amendments; and

- Order dated August 27, 2009 (the Order) detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities, as issued by the Government of India; and

- RBI guidelines dated September 17, 2009

  According to the guidelines dated September 17, 2009, issued by RBI, the entity will ensure meticulous compliance of the Order.

If the particulars of any of any customers matches those appearing in the list, the Company has to report those individuals to RBI/Financial Intelligence Unit-INDIA, New Delhi.

The details of the two lists are as under:

a) The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at:

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at:

https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

https://www.un.org/securitycouncil/sanctions/1988/materials

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

4.10 Key Appointments

4.10.1 Designated Director

A Designated Director means a person designated by the Company to ensure compliance with the obligations imposed under the PML Act and Rules. The Designated Director shall oversee the compliance position of AML norms and perform various functions as required under this Policy.

4.10.2 Principal Officer

The Company will appoint a Principal Officer, other than the person appointed as Designated Director, who will be a senior management official. The Principal Officer shall be independent and report directly to the Risk Management Committee. Principal Officer is responsible for:

(a) monitoring KYC/AML compliance and implementation of this policy;

(b) escalation of suspicious transactions reported by employees through STRs and submission of various reports to FIU-IND;

(c) sharing of information as required under the law.

They shall maintain close liaison with enforcement agencies, banks and any other institution that are involved in the fight against money laundering and combating financing of terrorism.

The Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

4.11 Other Compliances –

4.11.1 Central Know Your Customer Registry –

The Central KYC Registry (CKYCR) is responsible for electronically storing, safeguarding and retrieving KYC records and making them available online for all registered reporting entities. Reporting entities are required to register with the CKYCR in order to access or retrieve information pertaining to customers. It will issue a KYC identifier ID for all customers. CNH Capital will ensure compliance with the CKYC norms as stipulated by the RBI and PML Rules from time to time.

Functions and obligations of the Company

The Company shall have the following functions and obligations:

A. Register with the CKYCR in accordance with the processes and instructions issued.

B. While commencing a financing-based relationship, the Company shall verify the identity of the customer and perform the initial due diligence of the customer. Electronic copy of the customer's KYC records and information (Individual & Legal Entities) will be filed with the CKYCR on best effort basis.

C. The Company shall within 10 (Ten) days after the commencement of an financing-based relationship with a client, file the electronic copy of the client's KYC records and customer information with the Central KYC Registry.

D. Upon receiving the KYC Identifier from the CKYCR, communicate the same to the client by email, letter or any other written communication mode as may be decided from time to time.

Where a customer already possesses and submits a KYC Identifier to the Company, it shall download the KYC records from the Central KYC Registry by using the KYC Identifier and shall not require a customer to submit the documents again unless:

a) There is a change in the information of the customer as existing in the records of Central KYC Registry;

b) The current address of the client is required to be verified;

c) It is necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

After obtaining additional or updated information from a client as specified above, the Company shall as soon as possible furnish the updated information to the Central KYC Records Registry.

E. The company shall not use the KYC data of a customer obtained from the Central KYC Registry for purposes other than verifying the identify or address of the client and shall not

transfer KYC records
or any information contained therein to any third-party unless authorised to do so by the client or by the Regulator or by the Director.

F. When the Company is the last entity which performed the last KYC verification or sent updated information in respect of a client it shall be responsible for verifying the authenticity of the identity or address of the client.

4.11.2 Hiring and Training of Employees

The Company will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel.

The Company staff will be adequately knowledgeable about KYC/AML/CFT procedures. Specific training will be developed and implemented to ensure compliance in this area to all categories of staff.

The Company will conduct KYC/AML/CFT trainings/seminars at regular intervals so that there is necessary awareness of the Company's obligations under KYC/AML/CFT Regulations.

4.11.3 Adherence to KYC guidelines by persons authorised by the Company including agents

- Persons/entities authorised by CNH Capital for facilitating KYC process shall fully comply with provisions of this Policy. The Company shall include all relevant responsibilities in the agents' contracts and shall provide ongoing trainings for ensuring compliance with this policy.
- All information shall be made available to the RBI to verify the compliance with the KYC Policy and accept full consequences of any violation by the persons authorised by CNH Capital including agents who are operating on its behalf.
- The books of accounts of persons authorised by CNH Capital including agents shall be made available for audit and inspection whenever required.

5 REVIEW OF POLICY

The Principal Officer will review and assess the adequacy of this Policy annually or as required from time to time and recommend changes to the Board for the approval(s).

6 APPROVAL

The Policy has been approved by the Board of Directors of the Company in its meeting held on June 29, 2021.

APPENDIX 1 – BENEFICIAL OWNER

Beneficial Owner (BO) shall mean a person as defined below:

a. **Where the customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through on or more juridical person, has / have a controlling ownership interest or who exercise control through other means. For the purpose of this sub-clause-

   1. "Controlling ownership interest," means ownership of / entitlement to more than 25 per cent of the shares or capital or profits of the company.

   2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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

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

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

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

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

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

APPENDIX 2– LIST OF KYC

DOCUMENTS TO BE ACCEPTED FROM CUSTOMERS FOR THE PURPOSE OF IDENTIFICATION AND VERIFICATION

The Company shall obtain the following information from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

Individuals

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or

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

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

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

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

Where the customer has submitted,

i) Aadhaar number under clause (a) above to the Company notified under first proviso to sub-section (1) of section 11A of the PML Act, the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Company.

ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.

iii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annex I**.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under **Annex I.**

Provided that for a period not beyond such date as may be notified by the Government for a class of Banks, instead of carrying out digital KYC, the Bank pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD from the customer.

CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits his a proof of possession of Aadhaar Number containing Aadhaar Number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

NOTE: Till such time, the Company obtains requisite permission from UIDAI for eKYC authentication process, it shall obtain the OVD from the individual clients and verify from the originals.

Accounts opened using OTP based e-KYC, in non face to face mode are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.
ii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
iii. The aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.
iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out (Section of Master Direction – KYC Direction, 2016), If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
i. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
ii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in nonface-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
iii. Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above mentioned conditions.

Sole Proprietorship Firm

Where the client is a sole proprietorship firm, the certified copies of the following documents shall be submitted:—

(i) Any two of the following documents as a proof of business/ activity in the name of the proprietary firm:

(a) Registration certificate
(b) Certificate/license 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 / License/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, and landline telephone bills.

(ii) Customer due diligence of the individual (proprietor) shall be applicable, as applicable to an individual customer.

Hindu Undivided Family (HUF)

Where the client is an HUF, the certified copies of the following documents shall be submitted:

I. Identity Proof of the HUF

(i) PAN Card in the name of HUF and
(ii) Identification information of Karta and Major Co-Parcenors, as applicable to an individual customer.

And

II. Address Proof of the HUF

(i) IT returns filed by the HUF or
(ii) Bank Statement in the name of the HUF

And

i. **KYC as per Individual for the Karta**

Company

Where the client is a company, the certified copies of the following documents shall be submitted:—

(i) Certificate of incorporation;
(ii) Memorandum and Articles of Association;
(iii) Permanent Account Number of the Company
(iv) A resolution from the Board of Directors and power of attorney granted to the company's managers, officers or employees to transact on the company's behalf;
(iv) Identification information as applicable to individuals in respect of managers, officers or employees holding an attorney to transact on its behalf
(v) Such other document as may be required by CNH Capital

Partnership Firm

Where the client is a partnership firm, the certified copies of the following documents shall be submitted:—

(i) registration certificate;
(ii) partnership deed; and
(iii)Permanent Account Number of the Partnership Firm

(iv) Identification information as applicable to individuals in respect of person/s holding an attorney to transact on the firm's behalf

(v)such other document as may be required by CNH Capital.

Trust and Foundation

Where the client is a trust, the certified copies of the following documents shall be submitted:—

(i) registration certificate;

(ii) trust deed; and

(iii) Permanent Account Number or Form No. 60 of the trust

(iv) Identification information as applicable to individuals in respect of person/s holding an attorney to transact on the entity's behalf

(v) Such other document as may be required by CNH Capital

Unincorporated association (including unregistered trusts/unregistered partnership firms) or a body of individuals (including societies)

Where the client is an unincorporated association or a body of individuals the certified copies of the following documents shall be submitted:—

(i) resolution of the managing body of such association or body of individuals;

(ii) Permanent Account Number or Form No. 60 of the unincorporated accociation or a body of individual;

(iii) power of attorney granted to him/them to transact on the entity's behalf;

(iv) Identification information as applicable to individuals in respect of person/s holding an attorney to transact on the entity's behalf;

(v) such information as may be required by CNH Capital to collectively establish the legal existence of such an association or body of individuals.

*Obtaining a certified copy by CNH Capital shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorized officer of CNH Capital in a manner prescribed by the RBI.

Additional conditions for KYC document collection

(a) An individual, who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and who does not submit Aadhaar or proof of application of enrolment for Aadhaar, the following shall be obtained:
i. certified copy of an OVD containing details of identity and address and
ii. one recent photograph

(b) In case the client referred to above who is eligible to be enrolled for Aadhaar and obtain a Permanent Account Number, does not submit the Aadhaar number or the Permanent Account Number / Form 60 at the time of commencement of a new relationship with CNH Capital, the client shall submit the same within a period of six months from the date of the commencement of the relationship.

(c) In case the client fails to submit the Aadhaar number and Permanent Account Number / Form 60 within the previously mentioned six months period, the said relationship shall cease to be operational until the time the Aadhaar number and Permanent Account Number is submitted by the client.

For the purpose of ceasing the operation in the account, only credits shall be allowed and the Company shall duly inform the customer about this provision while opening the account.

(d) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the client referred to above does not have current address of the client, the client shall submit an officially valid document to CNH Capital. In case the OVD furnished by the client does not contain updated address, the following documents shall be deemed to be OVD's for the limited purpose of proof of address:-

- utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- property or Municipal tax receipt;
- pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- 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 license agreements with such employers allotting official accommodation

The client shall submit Aadhaar or officially valid document updated with current address within a period of three months of submitting the above documents.

ANNEX I - DIGITAL KYC PROCESS

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

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

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

D. The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall put a water-mark in readable form having 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.

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

F. 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 water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

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

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

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with

the Company shall not be used
for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

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

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

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

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

APPENDIX 3 - INTRODUCTION OF VIDEO BASED CUSTOMER IDENTIFICATION PROCESS (V-CIP):

The Company may undertake V-CIP to carry out:

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

Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Appendix 2 of the Policy, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

iii) Updation/Periodic updation of KYC for eligible customers.

REs opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

i) The Company should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

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

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

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

i) The Company shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

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

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

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

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

vi) The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a. OTP based Aadhaar e-KYC authentication
b. Offline Verification of Aadhaar for identification
c. KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

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

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, THE Company shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.

vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

viii) The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

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

x) The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this Master Direction – KYC Direction 2016, shall also be applicable for V-CIP.

ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.
