KYC / AML / CFT Policy

<u>of</u>

<u>LivQuik Technology (India) Private Limited</u>

<u>(Approved by the Board in its meeting held on 9th September, 2021)</u>

Preface

Reserve Bank of India (RBI) on February 25, 2016 (bearing ref no. RBI/DBR/2015-16/18 DBR.AML.BC. No.81/14.01.001/2015-16) notified the Know your customer (KYC) Directions, 2016 (KYC Directions, 2016), inter alia, directing that every Regulated Entity shall have a Know your customer (KYC) Policy duly approved by the Board of Directors. These directions have been issued by the RBI in terms of the provisions of Prevention of Money-Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules 2005.

LivQuik Technology (India) Private Limited ("LivQuik") is essentially an Information Technology Service providing company which holds Licence from RBI for Semi-Closed prepaid Payment Instrument.

Accordingly, the following KYC Policy has been adopted by the Board on 9th September, 2021, superseding the existing KYC & PMLA Policy of the Company, as amended from time to time.

KYC - AMLPolicy-2021

INDEX

POLICY/GUIDELINES ON 'KNOW YOUR CUSTOMER' (KYC) NORMS AND ANTI MONEY LAUNDERING MEASURES.

1. "KNOW YOUR CUSTOMER" NORMS.

1.1. Know Your Customer (KYC) is the platform on which Regulated entities operates to avoid the pitfalls of operational, legal and reputation risks and consequential losses by scrupulously adhering to the various procedures laid down for opening and conduct of account.

1.2. Know Your Customer is the key principle for identification of any individual/corporate opening an account.

1.3. The customer identification should entail verification on the basis of documents provided by the custoer. The objectives of KYC are as under:

1.3.1. To ensure appropriate customer identification.

1.3.2. Monitor the transactions of a suspicious nature.

1.3.3. Obtaining protection Under Section 131 of Negotiable Instruments Act.

1.3.4. Satisfy that the proposed customer is not an un-discharged insolvent.

1.3.5. Minimize frauds.

1.3.6. Avoid opening of Benami account/accounts with fictitious name and addresses and

1.3.7. Weed out undesirable customers.

1.4. For the purpose of KYC policy a "Customer" means

1.4.1. A person or an entity having a business relationship(engaged in financial transaction or activity) .

1.4.2. One on whose behalf the account is maintained (i.e. the beneficial owner).

The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

The procedure for determination of Beneficial Ownership is as under:

(a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

Explanation: - For the purpose of this sub clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than twenty-five percent of 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;

(b) Where the client 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 fifteen percent of capital or profits of the partnership;

(c) Where the client 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 or entitlement to more than fifteen percent (15%) of the property or capital or profits of such unincorporated association or body of individuals;

Explanation: Term 'body of individuals' includes societies.

Where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of Senior Managing official.

(d) Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the Trust, the Trustee, the beneficiaries with fifteen percent (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;

Identification of Beneficial Owner:

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:

i) 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.

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

1.4.3. Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc., as permitted under the law and

1.4.4. Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Regulated entities, say, a wire transfer or issue of a high value demand draft as a single transaction.

1.4.5. As per the instructions of RBI vide their letter No. DoS.CO.RPG/ 3923/ 11.01.002/ 2002/ 2019- 20 dated December 20, 2019 as per Section 3 (a) (iv) of the Master Direction- Know Your Customer (KYC) Direction, 2016 and also the Rule 9(1)(a) of the PML (Maintenance of Records) Rules 2005, further in terms of amendments to PML rules carried out by Govt. of India in August 2019, Beneficial Owner once established, has to be identified in the same manner as an individual customer. Thus We are required to identify the beneficial owner and take all reasonable steps to verify his identity.

1.4.6. Further, RBI advised that FATF Recommendation 10(b) on AML/ CFT and the FATF [paper on the best Practices on Beneficial Owner ship for legal Persons (October 2019), available on the website of FATF (http://www.fatf-gafi.org/), may be referred to for further guidance on the identification of BO.

Digital KYC Process

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

B. The access of the Application shall be controlled 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 to its authorized officials.

C. It must be 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 shall put a watermark in readable form having CAF number, GPS coordinates, authorized official‘s name, unique employee Code (assigned) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

D. The Application 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.

E. 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.

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

G. 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 Aadhar / 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 Aadhar / e-Aadhaar.

H. 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 shall not be used for customer signature. There must be a check put in place that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

I. 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. . 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.

J. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer , 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.

K. The authorized officer shall check and verify that:-

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

2. live photograph of the customer matches with the photo available in the document.; and

3. all of the necessary details in CAF including mandatory field are filled properly.;

L. On Successful verification, the CAF shall be digitally signed by authorized officer of the 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.

RBI Guidelines on Video-KYC

The Reserve Bank of India issued a notification amending KYC norms in January 2020. This amendment permits Regulated Entities to complete the KYC process remotely using video technology with the following being mandatory:

- The consent of customers should be confirmed before the Video-based Customer Identification Process (V-CIP)
- The customer's live photo should be geo-tagged to confirm they are located within India
- The application for the video KYC must be developed by the regulated entities and made available at specific customer touch points. Third-party video platforms are not to be used.
- The video process can only be initiated from the lender's domain and should be stored safely and securely by the lending entity
- The application will only be accessed through a live OTP, time OTP, or log-in ID and password
- The documents required to complete the verification can be either captured by video or uploaded
- Only banks are permitted to use OTP-based Aadhaar e-KYC authentication or offline Aadhaar verification
- Non-banking entities are permitted to use only offline Aadhaar verification
- If a customer does not wish to use Aadhaar for verification, other documents which provide the required details must be provided, which are officially valid
- Documents that are uploaded onto the DigiLocker government platform can also be used

Why KYC is Important?

Know Your Customer (KYC) was introduced in 2002 by the RBI. It was made mandatory for regulated entities to complete the KYC of all customers by December 2005. It helps financial institutions to authenticate and verify the identity and address of customers. It helps to ensure that money laundering and other illegal activities are not carried out by individuals. KYC is a one-time process.

Benefits of Video-KYC

The benefits of video KYC for both lenders and customers are numerous:

- Customers don't have to be physically present during the verification process
- This will make the process more inclusive for people from rural areas
- It facilitates faster and smoother verification processes for a better customer experience during on-boarding
- The costs of carrying out compliance and verification processes is reduced for financial institutions
- The safety and security of documents is ensured with the elimination of middlemen or agents for document collection purposes

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

(a) V-CIP Infrastructure:

i) We should comply 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 Wallet own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should becompliant with relevant RBI guidelines.

ii) To 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 . 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 reportedas 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 inconformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services 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) 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 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 authorized official 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, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi locker

It shall ensure to redact or blackout the Aadhaar number in terms of Para 3.1.2.4.

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 thatno 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 Digi locker.

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

x) The authorized official 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) The ultimate responsibility for customer due diligence will be with the Company.

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 .

xiv) The procurement of Video CIP application, IT and other infrastructures shall be procured and will be integrated with solution,. Further the V-CIP application / app will be also be placed in the website to facilitate the prospect customers to on-board through Video-CIP.

xv) The entire V-CIP will be handled at a Centralized location including concurrent auditing of the V-CIP process and authorization of the CIFs.

xvi) (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 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 policy, 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.

3.1.7 Periodical Updation of KYC: Periodic updation of KYC of customer is carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

i) In terms to amendment to Section 38 of Master Direction on KYC, the following procedure is to be adopted for Re-KYC i.e., Periodic updation of KYC of customers:

Risk – based approach for periodic updation of KYC is to be adopted.

1) For Individual Customers:

a) 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 customers email-id registered , customers mobile number registered .,

b) 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 customers email -id registered , customers mobile number registered ,

c) Wallet Accounts of customers who were minor at the time of opening account on their becoming major: In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards ..

d) Customers other than individuals:

a) No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered .

b) Change in KYC information: In case of change in KYC information, We shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

ii) Keeping in view of the COVID-19 related restrictions in various parts of the country, RBI has advised that in respect of the customer accounts where periodic updation of KYC is due and pending, no restrictions on operations of such account shall be imposed till December 31, 2021, for this reason alone, unless warranted under instructions of any regulator/ enforcement

agency/court of law, etc.

However, we have to continue engaging with the customers for having their KYC updated in such cases.

Important Guidelines for Video-KYC

It is important to keep the following guidelines in mind during your video KYC to ensure that it is completed smoothly:

- Make sure your background is white in color
- There should not be anyone else in the frame
- Your face should be clearly seen on the call
- When displaying a document for the live capture, it should be displayed vertically from above
- Make sure your ‘'location’' feature on your device is turned on
- Make sure that the link to the video process directs to a website
- To ensure the authenticity of the process, you could ask the officer to display their identity card and note down their name and employee ID

2. CUSTOMER ACCEPTANCE POLICY (CAP)

2.1 NEW CUSTOMER ACQUISITION PROCEDURES

2.2. PRECAUTIONS TO BE TAKEN

While opening the account it should be ensured that:-

2.2.1. No Wallet account is opened in anonymous or fictitious/Benami name(s).

2.2.2. No Wallet account should be opened where we are unable (to verify the identity and/or obtain documents required or non-reliability of the data/information furnished to us) to apply appropriate CDD measures, either due to non - cooperation of the customer or non

- reliabity of the documents/ information furnished by the customer.

2.2.3 No transaction or account - based relationship is undertaken without following CDD procedure.

2.2.4. Before opening a new wallet account, it should be ensured that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. Circulars issued by RBI / GOI should be referred from time to time wherein the names of banned/terrorist individuals/organization etc. are notified. The name(s) of the prospective customer should be verified with the latest –List of Terrorist Individuals/Organization under UNSCR 1267(1999) and 1822(2008) on Taliban/Al-Qaida Organization‖ integrated with CBS for 100% match and for more than 90% match available at our ftp server and the path -ftp://centftp.cbi.co.in/public/aml.

2.2.5. In cases where the customer is permitted to act on behalf of another person/entity the circumstances should be clearly spelt out in conformity with the established law and practice of regulated entities as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

2.2.6 Risk Categorization of Customers: Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception . While considering customer‘s identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the customer.

2.2.7 The customer profile shall be prepared based on risk categorization, as detailed in Para: 9 of this Policy. Periodic review of risk categorization should be followed .

3. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

One of the objectives of the "KYC" norms is to ensure appropriate Customer Identification. Customer Identification means undertaking the process of Customer due diligence (CDD) i.e. identifying the customer and verifying his/her identity by using reliable, independent source of documents ,data or information.

Customer identification procedure is to be carried out at different stages i.e.

(a) while establishing a wallet based relationshipwith the customer.

(b) carrying out a financial transaction and

(c) when we a doubt about the authenticity / veracity or the adequacy of the earlier obtained customer / identification data.

(d) Carrying out any international money transfer operations for a person who is not an account holder

(e) 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 fifty thousand.

(f) When there is reason to believe that a customer (account- based) is intentionally structuring a transaction into a series of transactions below the threshold .

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

2.

a. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

b. Adequate steps are taken by LivQuik 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 without delay.

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 LivQuik.

3.1 IDENTIFICATION OF CUSTOMER

Identification of a customer is an important pre-requisite for opening a wallet account. No Account is opened for any person without proper verification of the identity of the person. Careless handlingof the matter may give room forum desirable customers to commit frauds and misappropriation. Necessary precaution and strict adherence of norms in this respect can be a check on the activities of miscreants trying to defraud the regulated entity System.

Video based Customer Identification (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorized official for opening an account by undertaking seamless, secure, real-time, 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 process **complying with prescribed standards and procedures** shall be treated **on par with CIP** process.

3.1.1 WHAT IS IDENTITY?

Identity generally means a set of attributes which together uniquely identify a‘ natural‘ or a

_legal‘ person. The attributes which help in unique identity of a‘ natural‘ or _legal‘ person are called ‒identifiers‖. Identifiers are of two types: (A) Primary and (B) Secondary.

A) Primary Identifiers : Means and includes name (in full), Father‘s name, Date of Birth, Passport number, Voter Identity Card, Driving License, PAN number etc. as they help in uniquely establishing the identity of the person.

B) Secondary Identifiers: Includes address, location, Nationality and other such identification, as they help further refine the identity. The customer identification does not start and end at the point of application but it is always an ongoing exercise.

3.1.1.1. **Natural Person:**A natural person's identity comprises his name and all other names used, the date of birth, and an address/location at which he/she can be located and also his/her recentphotograph.

3.1.1.2. **Legal Person:** The legal status of the legal person/entity should be verified through proper and relevant documents; verify that any person purporting to act on behalf of the legal person /entity is so authorized and identify and verify the identity of that person ,understand the ownership and control structure of the customer and determine who are the natural person(s) who ultimately control the legal person.

The identity of a legal/corporate person comprises its name, any other names it may use, anddetails of its registered office and business addresses.

3.1.2 WHAT IS IDENTIFICATION?

3.1.2.1. Identification is the act of establishing who a person is.

3.1.2.2. In the context of KYC, identification means establishing who a person purports to be.

3.1.2.3. This is done by recording the information provided by the customer covering the elements of his identity (i.e. name and all other names used, and the address at which they can be located).

3.1.2.4. For undertaking CDD, the following shall be obtained 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. The features to be verified and the documents to be obtained for establishing identity of a person/customer are as under:-

Features	Documents

Accounts of Individuals • Legal name and Any other names used • Correct permanent address	A. Permanent Account Number (PAN) or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time and such other documents including in respect of financial status of the customer, or the equivalent e-documents thereof as may be required along with: B. Certified copy of any –Officially Valid Document‖ (OVD) or the equivalent e-document thereof containing the details of identity and address. **"Officially Valid Document" (OVD) means** i) the passport, ii) the driving licence, iii) proof of possession of Aadhaar number, iv) the Voter's Identity Card issued by the Election Commission of India, Provided that, a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:- i. Utility bill which is not more than two months old of any

	service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. Property or Municipal tax receipt; iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments,

	statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and v. Leave and licence agreements with such employers allotting official accommodation; c. Provided that the customer shall submit OVD with current address within a period of three months of submitting the documents specified at _b' above The additional documents mentioned above shall be deemed to be OVDs for the _low risk' customers for the limited purpose of proof of address, where customers are unable to produce any OVD for the same. d. A document shall be deemed to be an _Officially Valid Document' 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 a Gazette notification indicating such a change of name, while establishing an account based relationship or during periodic updation exercise, for persons whose name is changed due to marriage or otherwise. **When Aadhaar number is received from customers through electronic form ,** 1) We may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India (UIDAI) 2) Provided that in cases where successful authentication of Aadhaar number using e-KYC facility has been carried out, the other OVDs and photograph need not be submitted by the client.

	3) We shall carry out offline verification where offline verification can be carried out on the proof of possession of Aadhaar. –Offline verification‖ means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the regulations of UIDAI. Where customers submits their Aadhaar , We have to ensure such customers to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required. (Last 4 Digits can be visible) For equivalent e-document of any OVD, we can verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues there under and take a live photo as specified under Annex I. Any OVD or proof of possession of Aadhaar number where offline verification cannot be carried out, we can 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, instead of carrying out digital KYC, we 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. Any exception handling should be maintained separately . The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing the exception and additional details, if any. The database shall be audited periodically by Internal audit .

	This is purely when you enter in to an agreement with any corporate as most of the processes will be Retail
Accounts of Companies • Name of the Company • Principal place of Business. • Mailing address of the company • Telephone/Fax Number	For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: a) Certificate of incorporation; b) Memorandum and Articles of Association; c) Permanent Account Number of the Company d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and e)Documents specified for CDD procedure for individuals includes obtaining Aadhaar or any officially valid document or the equivalent e- document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60relating to the beneficial owner, the managers or employees as the case may Be holding an attorney to transact on the company‘s behalf.

3.1.2.5 Accounts of Politically Exposed Persons (PEPs):

a. Politically exposed persons 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. The identity of the person

is to be verified before accepting PEP as the customer. The decision to open an account for PEP should be taken at a senior level. They should also subject such accounts to

enhanced monitoring on an ongoing basis. Sufficient information including information about the sources of funds, accounts of family members and close relatives is to be gathered on the PEPs. The above norms may also be applied to the accounts of the family members or close relatives of PEPs and where PEP is the beneficial owner.

b. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, We should obtain senior management approval to continue the business relationship

3.2 Customer Due Diligence (CDD) :

The customer due diligence means identifying and verifying the customer and the beneficial owner. It may be defined as any measure undertaken by a financial institution to collect and verify information and positively establish the identity of a customer.

There are 3 types of CDD that can be used in accordance with the risk category of the customer.

3.2.1 Basic Due Diligence:

Basic Due Diligence means collection and verification of identity proof, address proof and photograph to establish the identity of the customer. This is based on documents and forms the basis of the KYC programme . A different set of documents can be listed for different type of customers as seen in Para 3.1.2.4. of this Policy.

3.2.2 Simplified Due Diligence:

The due diligence applied to establish the identity of the customer involving measures less stringent than Basic Due Diligence, can be termed as Simplified Due Diligence. Simplified Due Diligence can be applied to Accounts of people belonging to low income group.

3.2.3 Enhanced Due Diligence (EDD):

Additional diligence measures undertaken over and above the Basic Due Diligence can be termed as Enhanced Due Diligence. EDD would be required to be undertaken as per Reserve Bank of India guidelines for the medium and higher risk customers .

3.3 Guidelines on Aadhaar to be accepted as an –Officially Valid Document‖ under PML Rules

3.3.1 –Aadhaar number Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by udergoing the process of enrolment. As perAadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016); –Aadhaar number‖ means an identification number issued to an individual based on receipt of the demographic information and biometric information and after verifying the information by the Aadhaar issuing Authority, in such manner as may be specified by regulations, shall issue an Aadhaar number to such individual.

3.3.2 –Authentication‖, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 which is the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

3.3.3 –Digital KYC‖ means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer as per the provisions contained in the Act.

3.3.4 –Digital Signature‖ shall have the same meaning as assigned to it in clause (p) of subsection

(1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

3.3.5 –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.

3.3.6 Aadhaar number can be submitted by a customer where,

(a) he decides to submit his Aadhaar number voluntarily ;

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

(c) the proof of possession of Aadhaar number where offline verification cannot be carried out. (e)Authentication shall be carried out of the customer‘s Aadhaar number using e-KYC

authentication facility provided by the Unique Identification Authority of India

Explanation 1: We shall , where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required. Only 4 Digits should be visible

Explanation 2: Biometric based e-KYC authentication can be done

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, 2016 and the regulations made thereunder.

Guidelines on Unique Customer Identification Code (UCIC)

3.3.7 The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within and across the financial system.

3.3.8 Unique identifiers for customers has been introduced .

3.3.9 The existing customers having multiple CIFs are being consolidated by the exercise of de-duplication.

3.3.10 The UCIC will also help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable to have a better approach to risk profiling of

customers. It would also smoothen regulated entity operations for the customers.

3.4 <u>CDD Procedure and Sharing KYC information with Central KYC Records Registry (CKYCR) - Roll out of Legal Entity Template & other changes:</u>

(a) Govt. of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) to act as and perform the function of CKYCR vide Gazette Notification No. S.O. 3183 (E) dated 26th November 2015. ‑Central KYC Records Registry‖ means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. As per the 2015 amendment to PML (Maintenance of Records) Rules, 2005, we shall capture the KYC information pertaining to all new wallet opened for sharing with CKYCR in the manner mentioned in the rules, as per KYC templates finalized by CERSAI and as instructed vide our Circulars in this regard. The KYC records received and stored by the CKYCR could be retrieved online by any reporting entity across the financial sector for the purpose of establishing an account based relationship.

‑KYC Templates‖ means templates prepared to facilitate collating and reporting the KYC data to the CKYCR for individuals and legal entities.

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

(b) In terms of provision of Rule 9(1A) of PML Rules, we shall capture customer‟s KYCrecords and shall upload it onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI and we shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for „Individuals‟ and „Legal Entities‟ (LEs), as the case may be.

The templates may be revised from time to time, as may berequired and released by CERSAI.

(d) KYC records pertaining to accounts of Legal Entities (Non-Personal) opened on or after April 1, 2021, shall be uploaded with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

(e) Once KYC Identifier is generated by CKYCR, it shall ensure that the same is communicated to the individual/Legal Entities as the case may be.

(f) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the KYC data pertaining to accounts of individual customers and Legal Entities opened prior to 01.01.2017 and 01.04.2021 respectively shall be uploaded / updated, at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

(g) It shall be ensured that during periodic updation, the customers are migrated to the current CDD standard.

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

i. there is a change in the information of the customer as existing in the records of CKYCR;

ii. the current address of the customer is required to be verified;

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

3.5 Compliance of KYC policy: Ensuring compliance with KYC Policy through: (i) Specifying as to who constitute _Senior Management' for the purpose of KYC compliance. A Senior officer in the company shall be nominated for the purpose of KYC compliance. (ii) Allocation of responsibility for effective implementation of policies and procedures. The Designated Nodal Officer is designated as Compliance Officers. (iii) Independent evaluation of the compliance functions of policies and procedures, including legal and regulatory requirements by Compliance Dept, (iv) Concurrent / internal audit system to verify the compliance with KYC/ AML policies and procedures and submit audit notes and compliance to the Audit Committee. (v) Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports.

It shall be ensured that decision-making functions of determining compliance with KYC norms are not outsourced.

5. ANTI MONEY LAUNDERING STANDARDS

Money Laundering is the process whereby proceeds of crimes such as drug trafficking, smuggling, terrorism, organized crimes, fraud and many other crimes are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds.

The technological advancements and introduction of New Technologies – Credit Cards /Debit Cards/Smart Cards/ Gift Cards/Mobile Wallet/ Net Banking/Mobile Banking/ RTGS / NEFT

/ECS /IMPS etc have facilitated on line transfer of funds and real time settlement between the Banks across the globe. This has helped money launderers to adopt innovative means and move funds faster across continents making detection and preventive action much more difficult. This calls for a dynamic approach in tracking the crime. The staff members must be vigilant in the fight against money laundering and must not allow to be used for money laundering activities. We should not become the party to violation of law. As such, preventing money laundering activities is the duty and responsibility of the our staff.

We should pay special attention to any money laundering and financing of terrorism threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. As we our engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds, We are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. We should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to due diligence and KYC measures.

5.1 MONEY LAUNDERING:

As per the Prevention of Money Laundering Act (PMLA) 2002, the offence of Money Launderingis defined as:

Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or isactually involved in any process or activity connected with the proceeds of a crime and projecting the same as a untainted property – shall be guilty of offence of Money Laundering. Money

Laundering is the process by which the criminals attempt to hide and disguise the origin and ownership of the proceeds of their criminal activities like drug trafficking, trafficking in women and children, murder, extortion, child pornography etc. _Proceeds of crime' means any property derived or obtained, either directly or indirectly by any person as a result of criminal activities relating to a scheduled offence or the value of such property. Money Laundering, therefore, besides being a Statutory or Regulatory requirement is also a moral responsibility for all the regulated entity employees.

Nomination of Designated Director:

We are required to nominate a Director on their Boards as –Designated Director‖, as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules.

–Designated Director –means a person designated by the Board to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes the Managing Director or a whole-time Director duly authorized by Board of Directors if the reporting entity is a company. In no case, the Principal Officer shall be nominated as the Designated Director. The name, designation and address of the Designated Director are to be communicated to the Director, FIU-IND. In addition, it shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions referred to in PML Rule.

Principal Officer:

–Principal Officer‖ means an officer nominated , responsible for furnishing information as per Rule 8 of the PML rules. Principal Officer is responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law / regulations. The name, designation and address of the Principal Officer are to be communicated to the Director, FIU-IND.

5.2 TERRORIST FINANCING:

Terrorists use similar methods for moving their funds. Some of the terrorist groups also indulge in criminal activities for funding their acts. However, there are two major differences between

Money Laundering and Terrorist Financing.

4.2.1 Whereas in the case of Money Laundering, the source of money is always through criminal activities while Terrorist Financing can be from legitimately obtained income.

4.2.2 It is difficult to identify terrorist funding transactions as more often terrorist activities require small amounts.

5.3 WIRE TRANSFERS:

We may use wire transfers as an expeditious method for transferring funds between accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

5.3.1 The salient features of a wire transfer transaction are as under:

a) Wire transfer is a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through ,by electronic means with a view to making an amount of money available to a beneficiary person .. The originator and the beneficiary may be the same person.

b) Cross-border transfer means any wire transfer where the originator and the beneficiary are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

c) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to affect the

wire transfer may be located in another country.

d) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order to perform the wire transfer.

5.3.2 Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting , investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank/regulated entity to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, We must ensure that all wire transfers are accompanied by the following information:

(A) CROSS BORDER WIRE TRANSFERS.

i) All cross-border wire transfers including transactions using credit or debit card must be accompanied by accurate and meaningful originator information.

ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator‘s

account number or unique reference number as at (ii) above.

(B) DOMESTIC WIRE TRANSFERS

i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name; address and account number etc.,

ii) If we have reason to believe that a customer is intentionally structuring wire transfer to several beneficiaries in order to avoid reporting or monitoring, we must insist on complete customer identification before effecting the transfer . In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be sent to Compliance Officer at ROs /Principal Officer for onward submission to FIU-IND.

iii) When a credit or debit card is used to effect money transfer, necessary informationas (i) above should be included in the message.

5.4 CHECK LIST FOR PREVENTING MONEY-LAUNDERING ACTIVITIES

The illustrative checklist for preventing money-laundering activities is as under:

5.4.1 A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country.)

5.4.2 A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where regulated entity secrecy laws facilitatelaundering of money.

5.4.3 A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer‘s business or history.

5.4.4 A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

5.4.5 A customer experiences increased wire activity when previously there has been no regular wire activity.

5.4.6 Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

5.4.7 A business customer uses or evidences of sudden increase in wired transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.

5.4.8 Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.

5.4.9 Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

5.4.10 Instructing to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

5.4.11 Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

5.4.12 Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

5.4.13 Periodic wire transfers from a person's account/s to account haven countries.

5.4.14 A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

5.4.15 A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold or that involve numerous transactions .

5.4 Money Laundering and Terrorist Financing (ML/ TF) Risk Assessment:

a) As per Section (5A) of Chapter II of the MD on KYC 2016, We are required to carry out ‗Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

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

b) The risk assessment by us shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc... Further, the periodicity of risk assessment exercise shall be determined by the Board, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

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

6. MONITORING OF TRANSACTIONS– ON-GOING DUE DILIGENCE :

To obviate the scope for frauds and prevent Money Laundering, regular monitoring and supervision of accounts is essential. By understanding the normal and reasonable activity of the customers, coupled with controlling the accounts effectively, risk can be reduced.

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

Monitoring customer activity and transactions throughout the relationship helps us to know their customers, assess risk and provides greater assurance that we are not being used for the purposes of financial crime. However, the extent of monitoring shall be aligned with the risk category of the customer. High risk accounts have to be subjected to more intensified monitoring.

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

(a) Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being _washed' through the account.

(b) Special attention should be paid to the complex, unusually large transactions transaction and all unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or lawful purpose.

(c) Transaction which exceeds the threshold prescribed for specific categories of accounts.

A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be undertaken.

–Transaction‖ means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

(i) Opening of an account;

(ii) Deposits, withdrawal, or transfer of funds in whatever currency, or by electronic or other non-physical means;

6.1 MONITORING OF CASH TRANSACTIONS: Permanent account number (PAN) of customers shall be obtained and verified from the verification facility of the issuing authority while

undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks/ regulated entity ,as amended from time to time.

6.1.1. To effectively track the cash transactions We should monitor the details of individual deposits and withdrawals on following parameters:

Date of Transaction

Type of account/account no.

Title of account/Name of account holder
Date of opening the account

Amount of Deposit/withdrawal

Identity of the person undertaking the transaction

Name of the beneficiary

Destination of the funds

6.1.2 We have to review on receipt of these statements from the respective department and should immediately scrutinize the details thereof. In case any of the transactions prima-facie appears to be dubious or gives rise to suspicion, such transactions should be looked into by deputing officials . If any of the transaction is found to be of suspicious nature, it should be immediately informed to the Compliance cell and CEO .

6.1.3 Under the Prevention of Money Laundering Act' 2002 (PMLA) and Rules notified there under impose an obligation to verify identity of clients, maintain records and furnish information of details of the following transactions on monthly basis on or before 15th of succeeding month.

DIT will generate CTR reports and provide the same in XML format on monthly basis, which are being filed online on FINnet site of FIUIND.

6.2 Monitoring of other transactions

6.2.1 We should closely monitor the newly opened accounts in the initial 3 to 6 months oftheir opening and track the transactions with the profile of the customer.

6.2.2 Wherever the request is received for change in Mobile number, loss of SIM Card, complaints of sudden inactivation or failure of mobile connection, We should subject such accounts through enhanced monitoring and multiple checks, including calling on such mobile number/land line number seeking confirmation through other modes like e- mail etc.

6.2.3 Any such incident should immediately be reported to Compliance Officer

7. Combating Financing of Terrorism:

Requirements/ obligation under International Agreements & Communication from International Agencies

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

Updated list of individuals and entities linked to ISIL (Da'esh), Al-Qaida and Taliban are available at:
https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
https://www.un.org/securitycouncil/sanctions/1988/materials

The UNSC press release(s) concerning amendments to the list are available at URL: https://www.un.org/press/en/2020/sc14195.doc.htm

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

(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.

As and when list of individuals and entities approved by Security Council Committee established pursuant to various United Nations‘ Security Council Resolutions (UNSCRs) are received from Government of India / Reserve Bank of India, the same has to be updated to ensure the consolidated list of individuals and entities as circulated by Reserve Bank of India is updated. The updated list of such individuals/groups/undertakings/entities associated with Al-Qaida (―ISIL (Da‘esh) &Al-Qaida Sanctions list‖) and the updated list of such

individuals associated with Taliban and entitiesand other groups and undertakings associated with Taliban (―1988 Sanctions list‖) consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.

Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Compliance Officer at ROs / Principal Officer for onward submission to FIU-INDapart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

As per the instructions from the Ministry of Home Affairs (MHA), any request for delisting is to be forwarded electronically to Joint Secretary (CTCR), MHA for consideration. Individuals, groups, undertakings or entities seeking to be removed from the Security Council's ISIL (Da'esh) and Al-Qaida Sanctions List can submit their request for delisting to an independent and impartial Ombudsperson who has been appointed by the United Nations Secretary-General. More details are available at the following URL: https://www.un.org/securitycouncil/ombudsperson/application.

7.2 In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. We are therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

7.3 As per the communication received from the Financial Action Task Force (FATF), the strategic AML / CFT deficient jurisdiction are divided into 3 groups as under:

7.3.1 Jurisdictions subject to FATF call on its members and other jurisdictions to apply counter measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdiction: Iran

7.3.2 Jurisdictions with strategic AML/CFT deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies as of February 2010. The

FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdictionviz; Angola, Democratic People's Republic of Korea (DPRK), Ecuador and Ethiopia.

7.3.3 Jurisdictions previously publicly identified by the FATF as having strategic AML/CFT deficiencies, which remain to be addressed as of February 2010: Pakistan, Turkmenistan and Sao Tome and Principe.

Further, special attention should be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF statements.

Further, there should be ongoing monitoring. The background and purpose of transactions with persons (including legal and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations (as

mentioned above), should be examined and if it appears that such transactions have no apparent economic or visible lawful purpose, the background and purpose of the transactions should be examined, findings to be recorded and all documents and the written findings should be retained and made available to Reserve Bank of India /other authorities, on request.

7.4 What is Suspicious Transaction?

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 reasonable ground of suspicion that it may involve the proceeds of a crime regardless of the value involved or

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

c) appears to have no economic rationale or bonafide purpose;

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

e) Further, when we are unable to verify the identity and / or obtain documents required or

non-reliability of the data /information furnished and is unable to apply appropriate customer due diligence measures and therefore believes that it would no longer be satisfied that it knows the true identity of the customer, besides taking a decision whether to continue the business relationship, should also file an STR with FIU-IND.

7.5.2. Attempts to avoid reporting/record-keeping requirements.

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

7.5.3. Certain suspicious funds transfer activities

Sending or receiving frequent or large volumes of cross border remittances.

8. REPORTINGREQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA (FIU- INDIA) UNDER PMLACT 2002

a. We shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referredto in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to directthem about the form of furnishing information and to specify the procedure and the manner of furnishing information.

b. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website http://fiuindia.gov.in. shall be made use of by the regulated entity which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data.

c. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Regulated entity shall not put any restriction on operations in the accounts where an STR has been filed and shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

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

8.1 The prevention of Money Laundering Act, 2002 (PMLA) forms the core legal framework put in place by India to combat Money Laundering and Terrorism financing. In terms of the rules notified under

PMLA Act 2002, certain obligations have been cast on us with regard to reporting certain transactions. The same are detailed here under:

(a) Suspicious Transaction Report (STR)
(b)Cross Border Wire Transfer Report CBWT)

8.1.1 Suspicious Transaction Report (STR):

8.1.4.1 All suspicious transactions whether or not made in cash, should be reported within 7 days of arriving at a conclusion that any transaction is of suspicious nature. It should be ensured that there is no undue delay in arriving at a conclusion whether or not a transaction is of suspicious nature and that the principal officer should record his reasons for treating any transaction or a series of transactionsas suspicious nature.

8.1.4.2 Utmost care has to be exercised while drafting the Grounds of Suspicion (GOS), as GOS is the most important part of STR. The GOS should clearly express **"Why"** the transaction or activity is unusual, unjustified, does not have economic rationale or bonafides , keeping in mind the Business and services rendered . Specific reference needs to be drawn to the customer's profile, apparent financial standing, past activity in the account, general pattern etc. An indicative list of Grounds of Suspicion is enclosed as Annexure III.

8.1.2 Cross Border Wire Transfer Reports (CBWT)

(a) We are required to maintain the record of all transactions including the record of all cross border wire transfers in foreign currency, where either the origin or destination of the fund is in India.

(b) Cross-border Wire Transfer Report (CBWT) for every month should be furnished to Director, FIU-IND by 15th of the succeeding month.

(c) The information is to be furnished electronically in the FIN-Net module developed by FIU-IND.

8.1.3 Delay in Reporting to FIU-IND

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

8.1.4 Attempted Money Laundering Transactions:

In case a transaction is abandoned / aborted by customers, on being asked to produce details

/ or to provide information, We should report all attempted transactions, even if not completed bycustomers irrespective of the amount of transaction, in STR.

8.1.5 Need to file Repeat STR:

In cases, where STR has been filed in a particular account and fresh alerts are observed in the same account, the following factors have to be considered to judge and to take a decision for filing a repeat STR.

8.1.8.1 Has any additional ground of suspicion which has not been reported earlier, beennoted observed?

8.1.8.2Is the alert value / volume/ frequency is substantially high as compared to the earlier?

8.1.6 How to deal with the reported accounts?

The accounts reported in STR should be classified as high risk and should be subjected to enhanced monitoring. If significant activity is observed in these accounts, a repeat STR may be sent. Further, the competent authority should take a decision regarding closure of such an account / accounts where STR is repeatedly reported. However, such customers should not be tipped off.

8.1.7 Tipping off the customer:

There are no restrictions as such on us to discontinue operations in an account, which was reported in STR, to FIU-IND. In case, any restrictions have been placed in any account, it should be ensured that there is no tipping off the customer at any level. Tipping off would mean informing/communicating to the customer that his/her/their account has been or would be reported for suspicious activity to the Regulators/FIU-IND. However, seeking information about a particular transaction as part of the due diligence, should not tantamount to tipping off. Mentioned hereunder are some suggestions to avoid tipping off, which should be complied with by the field functionaries.

8.1.10.1 Due diligence should be preferably by way of pretext sales calls.

8.1.10.2 No statement should be made, which cautions or warns the customer.

8.1.10.3 AML triggers/rules/reporting thresholds and internal monitoring processes should

not be discussed with them.

8.1.10.4 The conclusion that has been arrived at after making the necessary enquiries should not be revealed .

8.1.10.5 No disclosure should be made to the customers that his/her accounts are under monitoring for suspicious activities or that STR has been filed/is being filed againsthim/her.

8.1.8 Procedure of STR Alerts scrutiny:

8.1.11.1 The STR alerts, based on scenarios, are generated through AML software (AML system). A team of front line officers at AML-KYC Cell are screening the generated STR alerts. After first level checking by a Senior Manager and secondlevel checking by Chief Manager, the suspicious alert shall be put up before the Principal Officer for his approval to file an STR to FIU-IND by AML Cell, CO,uploaded electronically on its FINnet site.

Indicative guidelines given to Front line Officers (MLRO) for monitoring of alerts:-

i. There is cyclic movement of funds between different parties

ii. There is high activity newly opened wallet accounts.

iii. There is sudden high activity in an account which is in-operative

8.1.11.2 Designated officers will scrutinize Money Laundering Reporting Officer (MLRO) for scrutiny of STR alerts . The Compliance Head looking after the functions of who is responsible for implementation of instructions issued on KYC-AML. He shall also act as first level checker for the screened STR alerts/referred probable STR cases and report to CEO

8.1.11.3 The Compliance Officer will monitor the effective and authentic screeningof STR alerts and remarks put for closure of STR alerts.

9. RISK MANAGEMENT

9.1. Identification of a customer is important pre-requisite for opening an account. Non-adherence of this may lead to the risks viz. frauds, money laundering, inadvertent overdrafts, Benami / fictitious accounts.

9.2. Non-compliance of monitoring of the transactions exceeding the threshold limit and non-recording of the transactions may result in intentional splitting/structuring of transaction to evade taxes, money laundering and financing of terrorist activities.

9.3. Risk Categorization of Customers

Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception .We should prepare the profile of the customer which should contain information relating to customers' identity, social/financial status, nature of business activity, information about his clients' business and their location etc. and risk categorization shall be undertaken based on these parameters. While considering customer‘s identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the customer .The customer profile shall be prepared based on risk categorization, as defined below:

9.3.1 Low Risk Category: Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.

Example:

a) Salaried Employees, whose salary structures are well defined,

b) People belonging to lower economic strata of the Society whose accounts show small balances and low turnover,

c) Government departments and Government owned Companies, Regulators and statutory bodies etc.

d) All other Customers who are not classified as High Risk or Medium Risk Categories

For low risk category customers, only the basic requirements of verifying the identity and location of the customer are to be obtained. However, whenever there is suspicious of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact pose a low risk, full scale customer due diligence should be carried out before opening an account or whenever such risk perceived.

9.3.2 Medium Risk Category: The Risk Classification may be lower for those customers where sufficient knowledge in the public domain is available

INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

i. Stock brokerage
ii. Import / Export
iii. Travel agency
iv. Used car sales
v. Telemarketers
vi. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
vii. Dot-com company or internet business
viii. Pawnshops
ix. Auctioneers
x. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
xi. Lawyers / Notaries (small, little known)
xii. Secretarial Firms (small, little known)

High Risk Category: Individuals and entities whose identities and sources of

funds are notclear and cannot be easily identified.

Example:

a) High Net Worth individuals

b) Trusts, Charities, NGOs and Organizations receiving donations(especially those operating on a ―cross border basis) unregulated clubs and organizations receiving donations. However, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.

c) Companies having close family shareholding or beneficial Ownership

d) Firms with 'Sleeping Partners'

e) Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which PEP is the ultimate beneficial owner;

f) Non face to face customers and

g) Those with dubious reputation as per public information available etc.

h) Customers dealing in antique goods

i) Money Exchange Bureaus

j) Diamond, Bullion Dealers &Jewellers

k) Arms and Ammunition dealers

Additional indicative list of High Risk Customers:

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.

ii. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities

iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations

iv. Individuals and entities specifically identified by regulators, FIU and other

competent authorities as high-risk

v. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.

vi. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.

vii. Accounts of Embassies / Consulates;

viii. Off-shore (foreign) corporation/business

ix. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale

x. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence

xi. Investment Management / Money Management Company/Personal Investment Company

xii. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.

xiii. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc

xiv. Money transfer Service Business: including seller of: Money Orders / Travelers‟ Checks / Money Transmission /Check Cashing / Currency Dealing or Exchange

xv. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)

xvi. Gambling/gaming including ―Junket Operators‖ arranging gambling tours

xvii. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).

xviii. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.

xix. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.

xx. Customers that may appear to be Multi-level marketing companies etc.

9.3.3.1 For High Risk Category & Medium Risk Category customers, the Enhanced Due Diligence (EDD) be done by taking the information such as customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. should be obtained. There should be periodical review of risk categorization of accounts followed by enhanced due diligence measures. Such review of risk categorization of customers should be carried out at least once in every six months.

9.3.3.2 We may take a view on risk categorization of each customer into low, medium and high risk category depending on their experience, expertise in profiling of the customer based on their understanding, judgment, assessment and risk perception of the customer and not merely based on any group or class they belong to.

10. INTERNAL CONTROL

To avoid such risks, we should put in place proper monitoring machinery to ensure that the AML risks are meticulously following the laid down guidelines/procedures with regards to KYC norms and Money Laundering activities.

10.1 Internal Audit/Inspection

10.1.1 Internal Auditors/Concurrent Auditors will carry out an independent evaluation of the controls, for identifying high value transactions.

10.1.2 **Concurrent / internal auditors will verify the compliance with KYC/AML policies and procedures.** They will specifically scrutinize and comment on the observance of KYC norms and the steps taken towards prevention of Money Laundering . As per the directions of DFS, GOI, 1% of the new accounts opened during the month/audit period be got verified by the Auditors by

reaching out to the new customers.

10.1.3 All accounts opened through V-CIP shall be made operational only after being subject to audit, to ensure the integrity of process .To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application shall be carried out before rolling it out .

10.3.1 STR reported accounts

Our KYC instructions stipulate –The accounts reported in STR bears a high degree of Risk and these accounts are subject to enhanced monitoring. If significant activities are observed in these accounts a repeat STR may also be filed. The competent authority should take a decision for closureof such an account/s where STR is repeatedly reported. However such customer should not be tippedoff.

Looking to the potential risk in such accounts, CEO Officer is designated as the appropriate authority to take decision for closure of such account in which more than **THREE** STRs have been filed.

10.5. <u>Preservation of Record/ Record Management</u>

10.5.1 All financial transactions records should be retained for at least five years from the date of transaction in terms of sub-section 2(b) of section 12 of the PML Act, the records referred to in clause(c) of subsection(1) of section12 shall be maintained for a period of five years from the date of cessation of transaction and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

10.5.2 In case of wire transfer/Electronic Funds Transfer transaction, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the account.

10.5.3 We should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like aadhaar, passports, identity cards, driving

licenses, PAN ,utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended.

10.5.4 The term ‑cessation‖ would broadly mean the closure of the account .However, there may be certain exceptions to this e.g.

10.5.4.1 If the matter related to a suspicious transaction is pending in a Court, the relevant records should be retained for 10 years from the date of final verdict ofthe Court.

10.5.4.2 In specific cases, where RBI/FIU-IND or any other regulatory body requests forthe retention of the records for a period more than 10 years, We should be guided by such requests.

10.5.5 The records pertaining to transaction and identification as mentioned above should be made available to the competent authorities upon request.

10.6. COMPLIANCE OFFICER/MONEY LAUNDERING REPORTINGOFFICER (MLRO)

10.6.1 The designated senior most officer to act as Compliance Officer. All suspicious transactions gets reported to the Compliance Officer immediately, who will investigate the suspicious transactions and report the same to the CEO.

10.6.2 COMPLIANCE OFFICER will initiate follow up action on unusual or suspicious activity and co-ordinate with their team in deciding on the desirability of continuing the account with increased caution and monitoring or to close the account.

10.6.3 The COMPLIANCE OFFICER will analyze the suspicious activities reported and track patterns ,which should be brought to the notice of the operating staff. This will enable the staff to remain vigilant against similar transactions.

10.6.4 Compliance officer can designate officers as Money Laundering Reporting Officer (MLRO) for scrutiny of STR alerts in case the STR alerts are decentralized for scrutiny .The MLRO will submit the report of scrutinized alerts to Compliance Officer for further Scrutiny and onward submission to CEO.

10.8 Hiring of Employees:

Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place to ensure high standards when hiring employees. We shall identify the Key positions within the organization structure having regard to the risk of money laundering and terrorism financing and the size of the business and ensure that the employees taking up such key positions are suitable and competent to perform their duties. – Detailed Policy on Hiring and HR duties and responsibility is part of the Information Security Policy

10.9Employee training:

On-going employee training is put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training is different for compliance staff, risk management staff, and Audit staff Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies, regulation and related issues also ensures its proper implementation.

10.10 Customer Education:

Implementation of AML/CFT measures requires us to demand certain information from customers which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/ income tax returns etc., this can sometimes lead to raising of questions by the customers with regard to the motive and purpose of collecting such information. There is, therefore, a need to sensitize their customers about these requirements as the ones emanating from AML and CFT frame work. We shall prepare specific literature/ pamphlets etc. so as to educate the customer\s of the objectives of AML/ CFTprocedures.

ANNEXURE- I

KNOW YOUR CUSTOMER (KYC) GUIDELINESANTI-MONEY LAUNDERING (AML) STANDARDS

KNOW YOUR CUSTOMER (KYC)			
Sr. No.	**DO"s**	**Sr. No.**	**DON"Ts**
1	Before onboarding any new customer account, it is ensured that the prospective account opener's identity does not match with any person with known criminal background, and his name does not appear in the list of terrorist individuals/ organizations banned by UN Security Council Sanction Committee as circulated by RBI.	1	Do not open account in anonymous or fictitious / benami name(s).
2	All the copies of supporting documents given by the customer must be verified with original documents.	2	Do not open account where we are unable to apply appropriate Customer Due Diligence (CDD) measures either due to non-cooperation of the customer or non – reliability of the documents / information furnished by the customer.
3	Circumstances in which a customer is permitted to act on behalf of another person / entity is clearly spelt out.	3	Do not accept new customer for relationship without application of CDD measures such as location of business activity / profession, purpose of the account, social and financial status source of funds etc.

4	Where PAN is obtained, the same shall be verified from the verification facility of the issuing authority.	4	Do not open any account without PAN or the equivalent e-document thereof or Form 60, a photograph and such other documents including in respect of financial status of the customer, or the equivalent e-documents thereof as may be required along with Proof of Identity and Address. Individuals –aadhaar or an officially valid document or the equivalent e-document thereof containing the details of his identity and address from the following: Passport, Driving License, Voter ID, Job Card issued by NREGA duly signed by officer of State Govt., Letter issued by the National Population Register or any document as notified by the Central Government in consultation with the regulator. Sole Proprietary Firm: Do not open account without CCD procedure of the proprietor along with any two documents or the equivalent e-document thereof as a proof of business / activity in the name of the proprietary firm- Registration certificate, Certificate/ licence issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST/VAT/ GST certificate (provisional / final) , Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, 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, 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 or Utility bills such as electricity, water, landline telephone

			bills, etc. Partnership Firm – Registration certificate, Partnership Deed, Permanent account number of the Partnership firm and documents specified for CDD procedure for individuals and includes obtaining aadhaar o any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60 relating to the beneficial owner, managers, officers or employees holding an attorney to transact on its behalf. Companies – Certificate of Incorporation, Memorandum and Articles of Association, Permanent account number of the company, Resolution of Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with documents specified for CDD procedure for individuals relating to the beneficial owner, for proof of identity and proof of address of managers, officers or employees holding an attorney to transact on its behalf. Trusts &Foundations-Registration certificate, Trust Deed, Permanent account number of Form 60 of the trust along with documents specified for CDD procedure for individuals relating to the beneficial owner for proof ofidentity and proof of address of the person holding a power of attorney to transact on its behalf. Unincorporated Association or Body of Individuals-Resolution of the managing body of such association or body of individuals, Permanent account number or Form 60 of the Unincorporated Association or Body of Individuals, Power of attorney granted to transact on its behalf alongwith documents specified for CDD procedure for individuals relating to the beneficial owner for proof of identity and proof of address of the person holding an attorney to transact on its behalf and any such information as may be required by the regulated entity to collectively establish thelegal existence of such an association or body of individuals. Juridical Persons: Government or its department, Societies,Universities and Local bodies like Village Panchayats -Documents showing name of person authorized to act onbehalf of the entity; along with documents specified for CDDprocedure for individuals relating to the beneficial owner for proof of identity and address in respect of the person holdingan

			attorney to transact on its behalf and Such documents as may be required by us to establish the legal existence of such an entity / juridical person.
5	All transactions of suspicious nature, should be monitored	5	Do not open an account without : Proof of either current or permanent address And the officially valid documents for proof of address and proof of identity.

6	Based on the risk perception, every new customer should be categorized into low, medium or high risk for monitoring purpose. Risk profiles of customers should be reviewed, once in every six months.	6	Services should not be denied to general public, especially, to those who are financially or socially disadvantaged.
7	Periodical updation of KYC information of every customer (including photographs) should be done every Two years for High Risk customers, every Eight years for Medium Risk customers and every Ten years for Low Risk customers.	7	In the accounts where a Suspicious Transaction Report (STR) has been made no restriction are put on the operations and it is ensured that there is no tipping off to the customers.
8	Proper record of all transactions reported to ZO/HO in CCR and STR formats are maintained/ preserved for a period of at least 5 years from the date of cessation of each such transaction.		
9	Where an equivalent e-document is obtained from the customer, We shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).		

ANNEXURE- II

For the benefit of every one, we are giving hereunder sample of GROUNDS OF SUSPICION reported in STRs

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable.
2	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
3	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected . The customer could not provide satisfactory explanation.
4	Unexplained large value/volume transactions inconsistent	Large Volume / value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.