FINO Payments Bank

KYC / AML /CFT Policy

Version 1.5

Revision history

Sr.no.	Summary of Change	Prepared By	Reviewed by	Approved by(Management Committee)	Approved by	Version No.	Effective Date
1	First Release	Sachin Shah, Team Member	K Hari Krishnan, Head, Risk Management, Compliance and Customer Grievances		Fino Payments Bank Board	1.0	April 29, 2017
2	The amendments have been suitably incorporated as per the regulatory instructions received from RBI.	Rimjhim Verma,Stella Bhattacharya, AML Department	K Hari Krishnan, Head, Risk Management Compliance and Customer Grievances	Standing Committee on Customer Service	Customer Service committee of the Board	1.1	April 26, 2018
3	1. Procedure for obtaining identification information is suitably appended under section 5.4.2 Customer identification procedure (CIP) as per Master Direction DBR.AML.BC.No.81/14.01.001/2015-16. 2. Transfer of accounts under section 5.4.2 has been deleted as it is not applicable as per the Bank's practice. 3. Updating KYC of minor accounts under section 5.4.2	AdityaRane,Stella Bhattacharya, AML Department	K Hari Krishnan, Head,Compliance and Customer Grievances	Standing Committee on Customer Service	Fino Payments Bank Board	1.2	February 11, 2019

	has been suitably modified as per Bank's practice. 4. Section 5.23.3 Counterfeit Currency Report (CCR) is suitably modified that Financial Intelligence Unit-India shall be reported in the specified format not later than 15th of the succeeding month pertaining to forged cash transactions or counterfeit currency notes or any forgery of a valuable security or document which has taken place for facilitating the transactions						
4	Amendment toMaster Direction on KYC BR.AML.BC.No.39/14.01.001/2018-19 dated May 29, 2019. Point number 1 to 6 suitably appended under section 5.4.2 Customer Identification Procedure (CIP). Point number 7 to 9 suitably appended under section 5.7 E-KYC procedures. Point number 10 to 12 suitably deleted from section 5.4.2 Customer identification procedure (CIP). Point number 13 suitably deleted from section 5.7 E-KYC procedures. 1) Proof of possession of Aadhaar Number 2) Aadhaar authentication/ offline-verification of an individual who voluntarily uses his Aadhaar number for identification purpose 3) Redact or blackout of customer Aadhaar number	Stella Bhattacharya, AML Department	K Hari Krishnan, Head,Compliance and Customer Grievances	Standing Committee on Customer Service	Fino Payments Bank Board	1.3	October 18, 2019

	4) For non-individual customers, PAN/Form No. 60 of the entity shall be obtained apart from other entity. 5) Closure of account in case of non-submission of PAN or Form 60. 6) Banks shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar. 7) For non-DBT beneficiary customers, Fino shall obtain a certified copy of any OVD containing details of his identity and address along with one recent photograph. 8) Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators. 9) Decision making functions of determining compliance with KYC norms shall not be outsourced. – clause deleted 10) Introduction shall not be sought while opening accounts- clause deleted 11) In case it is observed that the address mentioned as per 'proof of address' has undergone a change, the Bank shall ensure that fresh proof of address is obtained within a period of six months. Clause						

	deleted 12) Fino will print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal or e-KYC procedure as mentioned above shall be adopted, if such a customer knows only his/her Aadhaar number or if the customer carries only a copy of the e-Aadhaar downloaded from a place/source elsewhere.- clause deleted						
5	Master Direction – Know Your Customer (KYC) Direction, 2016 (Updated as on January 09, 2020). Digital KYC including Video based Customer Identification Process (V-CIP), Digital Signature; Equivalent e-document has been added in the policy. The missed amendments have been suitably incorporated as per the regulatory instructions received from RBI. 1) These guidelines on proprietorship concerns will apply to all customers with account opening date from June 01, 2019 – Clause modified in Customer Identification requirements (Accounts of Proprietorship Concerns). 2) Non-individual current account customers excluding proprietorship concerns (Individual) will be classified as medium risks. The risk classification may be lower for	S. Venkatanarayana, Stella Bhattacharya, AML Department	K Hari Krishnan, Head, Compliance and Customer Grievances	Standing Committee on Customer Service	Fino Payments Bank Board	1.4	January 27, 2020

	those customers where there is sufficient knowledge in the public domain available to the bank (e.g. listed companies, regulated entities, etc.) – Clause modified in Annexure II (ii Medium Risk) 3) In case PAN is not submitted, certified copy of an OVD (Officially Valid Document /OVD means the passport, the driving license, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and address) containing details of identity and address and one recent photograph shall be obtained. – Clause deleted from Customer Identification Procedure. 4) A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address. – Clause deleted from Customer Identification Procedure.						
6	Para 39 amendments on PAN or Form-60 updation and Temporary ceasing of operation from RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (Updated as on April 20, 2020) have been appended in	S. Venkatanarayana, Stella Bhattacharya, AML Department	K Hari Krishnan, Head, Compliance and Customer Grievances	Standing Committee on Customer Service	Fino Payments Bank Board	1.5	July 22, 2020

	the Customer Identification Procedure (para 5.5.2).						

Contents

1.Policy usage guide:

This section explains the structure of the policy document and the purpose of the same is to enable easy navigation and understanding of the contents of the document by various stakeholders. The Policy is organized in the following sections:

2.Regulatory reference

This section outlines the list of applicable regulations to the current policy document. The name of regulation issued by various regulators along with the date and reference number will be listed under this section. The purpose of the same is to enable various stakeholders in identification of applicable regulations for the policy and act as a ready reference for the regulations.

3.Key stakeholders and roles

Under this section, a list of all the key stakeholders involved in the design, review, approval and implementation of the policy are identified and the major roles to be performed by them are listed. This section enables various stakeholders in understanding their respective roles with regard to the current policy

3.1 Account Opening Executive

For e-KYC customers, the Aadhaar number of the customer needs to be captured and biometric information of the customer needs to be verified through the UIDAI server.

3.2 KYC Audit Team at CPU

Conducting KYC Audit on documents collected from customer e-KYC.

4.Frequently asked questions

This section lists down the frequently asked questions with respect to the current policy document from the perspective of various stakeholders and gives a reference to the relevant section of the policy to aid in clear understanding of the question.

4.1 What is Money Laundering and Financial Terrorism?

Money laundering refers to conversion of money illegally obtained to make it appear as if it originated from a legitimate source. Money laundering is being employed by launderers worldwide to conceal criminal activity associated with it such as drugs /arms trafficking, terrorism and extortion.

Financial Terrorism means financial support to, in any form of terrorism or to those who encourage, plan or engage in terrorism.

Money launderers send illicit funds through legal channels in order to conceal their criminal origin while those who finance terrorism transfer funds that may be legal or illicit in original in such a way as to conceal their source and ultimate use, which is to support Financial Terrorism.

4.2 What is KYC?

KYC is an acronym for “Know your Customer” a term used for Customer identification process.
It involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc which in turn helps the banks to manage their risks prudently.
The objective of the KYC guidelines is to prevent banks being used, intentionally or unintentionally by criminal elements for money laundering.

4.3 What is KYC Policy?

As per RBI guidelines, all banks are required to formulate a KYC Policy with the approval of their respective boards. The KYC Policy consists of the following four key elements:
1) Customer Acceptance Policy
2) Customer Identification Procedures
3) Monitoring of Transactions
4) Risk Management.

4.4 Who is a Customer?

For the purpose of KYC policy a ‘customer” may be defined as:

- A person or entity that maintains an account and/or has a business relationship with the bank;
- One on whose behalf the account is maintained (i.e. the beneficial owner);

- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say a wire transfer or issue of high value demand draft as a single transaction.

4.5What is a Customer Acceptance Policy?

Customer Acceptance Policy refers to the general guidelines followed by banks in allowing customers to open accounts with them. Generally the guidelines stipulate that no accounts shall be opened in anonymous or fictitious names or when the identity of the customer matches with any person with known criminal background or banned entities. Similarly accounts should not be opened when the bank is unable to verify the identity and/or obtain documents required as per the bank's policy.

4.6What is the Customer Identification Procedure?

Customer identification means identifying the customer and verifying his/her identity through reliable and independent documents, data and information. Banks would need to satisfy to the competent authorities that due diligence was observed in accordance with the requirements of existing laws and regulations.

4.7What are the features to be verified and documents required to be obtained from customers?

The features to be verified and documents that may be obtained vary depending upon the type of customers.

4.8When does KYC apply?

KYC will be carried out for the following but is not limited to:

- Opening a new account (deposit)
- Opening a subsequent account where documents as per current KYC standards not submitted while opening the initial account.
- When the bank feels it is necessary to obtain additional information from existing customers based on the conduct of the account.
- After periodic intervals based on instructions received from RBI.
- When there are changes to signatories, mandate holders, beneficial owners, etc.

5.Policy content

This section contains various aspects of the policy design and implementation as per the applicable regulatory guidelines. This section outlines the action required by various stakeholders of the Bank in ensuring implementation of the policy.

5.1 Purpose

RBI has advised Banks that a proper Policy on 'Know Your Customer [KYC]', 'Anti Money Laundering [AML]' and 'Combating of Financing of Terrorism [CFT]' measures and obligation of bank under Prevention of Money Laundering Act, 2002 be formulated and put in place.

The purpose of KYC/AML/CFT policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of

suspicious nature for the purpose of reporting to Financial Intelligence Unit India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) on AML standards and on CFT measures.
For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

5.2 Objective

The Policy has been framed to develop a strong mechanism for achieving the following objectives:

To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps them to manage the associated risks prudently.

To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC / AML / CFT measures / Obligation of Bank under PMLA 2002 and to cooperate with various government bodies dealing with related issues.

5.3 Definition of customer

For the purpose of KYC Policy, a 'Customer' is defined as:

- A person or entity that maintains an account and/or has a business relationship with the Bank and/or receives occasional/regular cross border inward remittances under Money Transfer Service Scheme [MTSS] and/or undertakes regular/occasional transaction with regard to purchase/sale of foreign currency notes/traveler cheques;
- One on whose behalf the account is maintained, i.e. the beneficial owner. [Beneficial Owner means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person];
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law;
- And any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

5.4 General Guidelines

Bank will ensure that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Bank will ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued for accepting customer & opening of accounts. Any other information required will be sought separately from the customer after opening the account.

Bank will ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rs.50,000/- [Rupees fifty

thousand] and above is effected by debit to the customer's account or against cheques and not against cash payment.

Bank will not make payment of cheques / drafts / pay orders / banker's cheques bearing that date or any subsequent date, if they are presented beyond the period of three months from the date of such instrument.

Bank will ensure that the provisions of Foreign Contribution (Regulation) Act, 2010 as amended from time to time, wherever applicable are strictly adhered to.

5.5 Four key elements of KYC policy

There will be four pillars of KYC policy, as under:

1. Customer Acceptance Policy;
2. Customer Identification Procedures;
3. Monitoring of Transactions; and
4. Risk Management

5.5.1Customer acceptance policy (CAP)

As a Customer Acceptance Policy, the Bank will verify the identity as laid down in Customer Identification Procedures and the Bank will:

- Not accept any person / entity barred by law of the land to avail banking facilities as its customer;
- Not open accounts in the name of anonymous or fictitious/benami person(s) or account on behalf of other persons whose identity have not been disclosed or cannot be verified. Bank will also not receive remittance/conduct transactions with regard to purchase/sale of foreign currency notes/ traveler cheques in respect of such persons;
- not open accounts of person(s) whose identity matches with any person with known criminal background or with banned entities such as individual terrorist or terrorist organizations etc;
- Not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or no reliability of the data/information furnished to the bank. The decision to close an account will be taken at the level of Incumbent In Charge of the branch after giving due notice to the customer, in writing , explaining the reasons for such a decision;
- Ensure to obtain documents and other information in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act 2002 and instructions/guidelines issued by RBI and Ministry of Finance, Deptt. Of Financial Services, Govt. of India from time to time;
- Parameterize risk perception of the customer in terms of nature of business/activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into three types of risk categories viz., Low, Medium and High Risk, based on risk perception decided on acceptance criteria for each category of customers;

- Not make payment of any remittance where the Bank is unable to apply appropriate customer due diligence measures i.e., the Bank is unable to verify the identity and/or obtain required documents as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished. In case the customer does not cooperate by furnishing necessary documents/information, the Bank may terminate relationship with the customer. However, it will be ensured that the customer is not harassed.
- The mandatory information sought for KYC purpose while opening of an account and during the periodic updation by the Bank needs to be complete and adequate. The 'Optional/ additional information to be obtained with explicit consent of the customer, prior to opening of the account
- Opening of a joint account needs to be as per the customer due diligence procedures
- Ensure that the Customer Acceptance Policy and its implementation does not become too restrictive resulting in denial of banking services to general public, especially to those who are financially or socially at a disadvantage position.
- Prepare a profile for each new customer based on risk categorization. The customer profile will contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority
- Where an equivalent e-document is obtained from the customer, Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000)

The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile bank will ensure that only such information is sought from the customer, which is relevant to the risk category and is not intrusive. The customer profile will be treated as a confidential document and details contained therein will not be divulged to outsiders for cross selling or any other purposes.

5.5.2 Customer identification procedure (CIP)

For undertaking CDD, Fino shall obtain the following information from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity: From an individual who is eligible for enrolment of Aadhaar, the following shall be obtained:

i. Aadhaar number; or Proof of possession of Aadhaar number
ii. Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
iii. Certified Copy" - Obtaining a certified copy by the Bank shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Bank as per the provisions contained in the Act.
iv. 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 authorised officer of the Bank as per the provisions contained in the Act.

v. 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).

vi. 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.

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

viii. Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

ix. Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the Bank by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

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

Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months.

Proof of possession of Aadhaar number can be obtained as one of the list of Officially Valid Documents (OVD) with a provision that where the customer submits 'Proof of possession of Aadhaar number' as OVD, he may submit it in such form as are issued by the Unique Identification Authority of India (UIDAI).

In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have current address, an OVD (Officially Valid Document /OVD means the passport, the driving license, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and address) shall be obtained from the customer for this purpose.

In case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

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

ii. property or Municipal tax receipt;

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

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

In such cases the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

Certified copy of OVD: comparing the copy of officially valid document with the original and record the same on the copy by the authorised officer of the bank

b) From an individual, who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and who does not submit Aadhaar or proof of application of enrolment for Aadhaar, the following shall be obtained:

i. certified copy of an OVD containing details of identity and address and

ii. one recent photograph

c) From an individual who is not eligible to be enrolled for an Aadhaar number, or who is not a resident, the following shall be obtained:

i. PAN or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time.

ii. one recent photograph and

iii. A certified copy of an OVD containing details of identity and address.

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

Fino may carry out Aadhaar authentication/ offline-verification of an individual who voluntarily uses his Aadhaar number for identification purpose.

Fino shall also ensure that the customers (non-DBT beneficiaries) while submitting Aadhaar for Customer Due Diligence, redact or blackout their Aadhaar number. Provided further that, while opening accounts of legal entities, in case, PAN of the authorised signatory or the power of attorney holder is not submitted, the certified copy of OVD of the authorised signatory or the power of attorney holder shall be obtained, even if such OVD does not contain address."

For non-individual customers, PAN/Form No. 60 of the entity (for companies and Partnership firms - only PAN) shall be obtained apart from other entity related documents. The PAN/Form No. 60 of the authorised signatories shall also be obtained.

In case of existing customers, Bank shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central

Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, Bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

If a customer having an existing account-based relationship with Fino and gives in writing to the Fino he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, the Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Fino shall duly inform the customer about this provision while opening the account. "

At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based)

Fino at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) .

Provided,

i. Where OTP based authentication is performed in ‘non-face to face’ mode for opening new accounts, the limitations as specified in E-kyc procedures shall be applied. Accounts opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per any of the Existing mode(like Physical document collection/Aadhaar authentication/ offline-verificationo/ Biometric using DBT).

ii. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators/ Biometric enabled ATMs"

The Customer Identification Procedure will be carried out at the time of:

- Establishing banking relationship;
- Carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
- Carrying out any international money transfer operations for a customer who is not an account holder of the bank.
- When the Bank feels it is necessary to obtain additional information from the existing customers based on the conduct/behavior of the account.

- The Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- Selling third party products as agents, selling their own products, sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
- Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- Not required for wallet accounts within RBI specified limits which require no KYC

The Customer Identification Procedure means:

- Identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.
- For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank at its option, rely on customer due diligence done by a third party, subject to the following conditions:
- Necessary information of such customers' due diligence carried out by the third party is immediately obtained by the Bank.
- Adequate steps are taken by the bank to satisfy 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.
- 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.
- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.
- Decision making functions of determining compliance with KYC norms shall not be outsourced.
- The nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons [individuals], the bank to obtain sufficient identification data to verify the identity of the customer, address/location, and also recent photograph. It has been decided that:
- Introduction shall not be sought while opening accounts
- If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the Account Opening Form (AOF), the document may be accepted as a valid proof of both identity and address. If the address indicated on the document submitted for identity proof differs from the current address mentioned in the AOF, a separate proof of address should be obtained.
- For customers that are legal persons or entities, the bank will:
- verify the legal status through proper/relevant documents;.
- For opening of an account of a company, one certified copy of each of the following documents shall be obtained:
- Certificate of incorporation.
- Memorandum and Articles of Association.
- A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.

- Officially valid documents in respect of managers, officers or employees holding an attorney to transact on its behalf.
- The list of documents to be obtained in the case of a partnership, trust and unincorporated association shall vary than that mentioned above.
- 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 persons who ultimately control the legal person;
- The information so collected will be used for verifying the identity of:
- the named account holder;
- the beneficial owners; However, in case of intermediaries (pooled) accounts, the customer due diligence process will include ensuring that these are regulated/supervised and/or having adequate systems in place to comply with KYC requirements;
- the signatories to an account; and
- the intermediary parties.
- Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc. will be collected for completing the profile of the customer.
- Bank will allot a Unique Customer Identification Code [UCIC] while accepting a customer. Each customer will be allotted one single Customer-Id and all the accounts will be attached to the Unique Customer Identification Code [Customer-Id].

This will help Bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable bank to have a better approach to risk profiling of customers and smoothen banking operations for the customers.

Bank will ensure that the multiple identities of the existing customers are clubbed together to have one single Customer-Id for each customer.

However the Bank shall not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

- In case there is suspicion of money laundering or terrorist financing or other factors, which give rise to a belief that the customer does not, in fact, pose a low risk, Bank will carry out enhanced customer due diligence (CDD) before opening an account.

In case there is suspicion of money laundering or financing of activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, Bank shall establish the identity of the customer through the production of “officially valid documents”.

Accounts of Close Relatives: For opening of accounts of the close relatives i.e. wife, son, daughter and parents, who live with their husband, father/mother and son, who find it difficult to open an account, as utility bills etc. for address verification are not in their name, the Bank will obtain the identity document of the prospective customer and the utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the prospective customer is staying with him/her. Bank will also obtain any other supplementary evidence such as a letter received through post for further verification of the address of the prospective customer.

- Bank will intimate their customers that in the event of change in address due to relocation or any other reason, they should intimate the new address to the bank within two weeks of such a change. While opening new accounts and while periodically updating KYC data, an undertaking to this effect should be obtained

- Updating of KYC Data:

- Bank will do full KYC exercise including obtaining fresh photograph/s at least every two years for high risk individuals/entities, at least every eight years for medium risk individuals/ entities and at least every ten years for low risk individuals/ entities.

- A certified copy of the proof of address forwarded by 'low risk' customers through mail/post, etc., in case of change of address shall be acceptable. Physical presence of low risk customer at the time of periodic updation shall not be insisted upon.

- As and when the Bank rolls out accounts for minors, Bank will obtain fresh photographs from minor customer on becoming major. Such Verification will be done irrespective of whether the account has been transferred from one branch to another and the Bank will maintain records of transactions as prescribed.

- (a) For periodic updation the Bank shall carry out following procedures:

i. PAN verification from the verification facility available with the issuing authority and

ii. Authentication, of Aadhaar Number already available with the Bank with the explicit consent of the customer in applicable cases.

iii. In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.

iv. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorised as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

v. In case of Legal entities, the Bank shall review the documents sought at the time of opening of account and obtain fresh certified copies.

- (b) Bank may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bonafides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.
- (c) The Bank shall ensure to provide acknowledgment with date of having performed KYC updation.
- (d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

- The nature and type of documents/information that may be relied upon for customer identification and for the purpose of proof of correct address and as enlarged in terms of the Department of Financial Services, Ministry of Finance Government of India. The permanent correct address means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the bank for verification of the address of the customer.

- Customer Identification procedure will also be carried out in respect of non-account holders approaching bank for high value one-off transaction.
- Branches will accept NREGA Job Card as KYC document for opening a 'normal account' duly signed by an officer of the State Government as a valid document for opening of bank accounts without the limitations applicable to 'Small Accounts'.
- While opening Bank accounts of an individual based on Aadhaar, Bank will satisfy about the current address of the customer by obtaining the required proof of the same as per extant guidelines. In case the address provided by the account is the same as that of Aadhaar letter, it may be accepted as a proof of both identity and address.
- The antecedents of prospective customer have to be verified to the satisfaction of the official authorized to allow opening the account, in addition to obtaining documents as prescribed. The introduction by an existing KYC compliant customer need not be insisted upon. However, the due diligence at the time of accepting a customer is of utmost importance to avoid frauds. Spirit of KYC norms is to ensure the authenticity of Identity and Address of the customer. A certificate of having verified genuineness of Voter's ID Card/PAN Card must be appended on the photocopy of the documents and kept with AOF.

5.6Types of customer due diligence

5.6.1 Basic Due Diligence [BDD]

Basic Due Diligence [BDD] implies collection and verification of identity proof, address proof and photograph to establish the identity of the customer.

For undertaking CDD, Banks shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) theAadhaar number where,

i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
ii. he decides to submit his Aadhaar number voluntarily to a bank or any Bank notified under first proviso to sub-section (1) of section 11A of the PML Act; or

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

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

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

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

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank or to a Bank notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or Bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.

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

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

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

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

Banks may undertake live V-CIP, to be carried out by an official of the Bank, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the Bank performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

   • Banks: can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP.

• REs other than banks: can only carry out Offline Verification of Aadhaar for identification.

ii. Bank 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the Bank shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the Bank shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. 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.

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. Bank shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. Bank shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the Banks shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the Bank itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. Banks shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. Banks are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Bank.

xiii. Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

xiv. BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

5.6.2 Simplified Due Diligence [SDD]

Any due diligence applied to establish the identity of the customer, which involves measures less stringent than basic due diligence can be termed as 'Simplified Due Diligence'. [SDD]. SDD can be applied to accounts of people belonging to low income group, both in urban and rural areas and can also be applied to 'Small Accounts' as given under paras.

5.6.3 Enhanced Due Diligence [EDD]

Any additional measures undertaken over and above the Basic Due Diligence can be termed as Enhanced Due Diligence, necessitating additional information on the customer/transactions. This is applicable for all High Risk Customers.

5.7Customer identification requirements

5.7.1 For Walk-in Customers:

Customer identification procedure will also be carried out in respect of walk-in customers (non-account based customer) approaching bank for transactions equaling or exceeding Rs.50, 000/- [Rupees fifty thousand], whether conducted as a single transaction or series of transactions that appear to be connected.

However, in case Bank has reason to believe that customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-, Bank will verify identity and address of customer and in case of suspicion may consider filing of Suspicious Transaction Report (STR) to FIU India.

Note: In terms of Prevention of Money Laundering Rules, 2005, Banks are required to verify identity of customers of all international money transfer operations.

5.7.2 Accounts of migratory workers:

In order to smoothen the process of opening of bank accounts by the migratory workers, who have no proof of current place of residence, the Ministry of Finance, Deptt.of Financial Services letter F.No.31/3/2011-BO.II dated 20th July, 2012 has issued instructions advising the following procedure for opening of bank accounts of migratory workers. The Bank will follow this procedure which is mentioned below:

- A migratory worker may visit any branch of the bank servicing the area of his / her permanent residence for opening a bank account;
- The branch will open his / her account/wallet on self-certification basis, or on introduction basis, and / or on the basis of the documents made available by the individual including a proof of permanent place of residence, as the case may be, and allow operations immediately; (Modification required)
- The bank while opening such an account/wallet, if required, may get the details / proof of permanent place of residence verified through an 'on-line' communication to the branch servicing the area of permanent domicile of the customer, within 30 days of opening of an account, within which the customer may be allowed operations as permissible for 'small account' to enable him / her to meet basic day-to-day requirements of funds;

- On receipt of ‘on-line’ verification of documents, the bank branch will allow full operational facilities in the account, which are available to a normal account.

5.7.3 Salaried Employees:

In case of accounts of salaried persons/employees, in order to minimize the risk of fraud, Bank will rely on certificate/letter of identity/address issued only by corporate and other entities of repute and will ascertain the competent authority designated by the concerned employer to issue such certificate/letter.

Further, in addition to the certificate from employer, the bank will obtain at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules e.g. passport, driving license, PAN Card, Voter’s Identity Card etc. or utility bills for KYC purposes for opening account of salaried employees of corporate and other entities.

5.7.4 Trust/Nominee or Fiduciary Accounts:

There may be possibility that the trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Bank will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the Bank will take reasonable precautions and will insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting and will also obtain details of the nature of the trust or other arrangements in place.

While opening an account for a trust, Bank will take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

In case, a 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 banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

5.7.5 Accounts of companies and firms:

Bank will exercise caution against business entities being used by individuals as a “front” for maintaining accounts with the Bank. As a check, Bank will examine the control structure of the entity, determine the source of funds and identify the natural persons who have controlling interest and who comprise the management.

These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

5.7.6 Accounts of Politically Exposed Persons (PEPs):

- Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public positions/functions in a foreign country, e.g., Heads of States or of

Governments, Senior politicians, Senior Government/Judicial/Military officers, Senior Executives of state-owned corporations, important political party officials etc.

- Bank will ensure enhanced due diligence and will gather sufficient information on any person/customer of the category of PEPs intending to establish a banking relationship and try to collect and check all information available on the person in the public domain.

- Bank will also verify the identity of the person and seek information about the sources of funds before accepting PEP as customer. Such accounts will be subjected to enhance monitoring on an ongoing basis.

- Decision to open an account including existing customers or the beneficial owner of an existing account subsequently becoming a PEP will be taken at Senior Management Level i.e. at the level of VP and above.

- In the event of existing customers or the beneficial owner of an existing account subsequently becoming a PEP, the approval of the officer of the Bank at a suitably higher level will be obtained to continue the business relationship and subject the account to the enhanced due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an on-going basis.

- The said norms will also apply to the accounts of the family members or close relatives of PEPs. Such type of Customers requiring very high level of monitoring will be categorized as 'High Risk'. These instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

5.7.7Accounts of juridical persons:

For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, a certified copy of the following documents shall be obtained:

- Document showing name of the person authorized to act on behalf of the entity;
- Officially valid documents for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and
- Such documents as may be required by the bank to establish the legal existence of such an entity / juridical person.

5.7.8Accounts of Proprietorship concerns:

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, bank will also verify & obtain any two of the following documents which should be in the name of proprietary concern:

- Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern),
- Certificate / license issued by the Municipal authorities under Shop & Establishment Act,

- Sales and Income Tax Returns,
- CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities,
- License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian
- Medical Council, Food and Drug Control Authorities,
- Registration /licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department.
- Importer Exporter Code(IEC) issued to the proprietary concern by the office of DGFT,
- The 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 and
- Utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern as required documents for opening of the bank accounts of proprietary concerns.

These guidelines on proprietorship concerns will apply to all customers with account opening date from June 01, 2019.

5.8 Digital KYC Process:

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

B. The access of the Application shall be controlled by the Banks 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 Banks to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.

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

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

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

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

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

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

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

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

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

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

Banks may use the services of Business Correspondent (BC) for this process.

5.9E-KYC Procedures:

The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification under the PML Rules, as

(a) The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document', and

(b) Transfer of KYC data, electronically to the Bank from UIDAI, is accepted as valid process for KYC verification.

Fino will obtain authorization from the individual user authorizing UIDAI by way of explicit consent to release his/her identity/address through biometric authentication to the Banks.

Banks shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016. Banks, at receipt of the Aadhaar number from the customer may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the UniqueIdentification Authority of India upon receipt of the customer's declaration that he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the AadhaarAct, 2016.

For non-DBT beneficiary customers, Fino shall obtain a certified copy of any OVD containing details of his identity and address along with one recent photograph.

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

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

(a) there must be a specific consent from the customer for authentication through OTP.

(b) the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh.

(c) the aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.

(d) accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure is to be completed. If the CDD procedure is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

(e) a declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC either with the same bank or with any other bank. Further, while uploading KYC information to CKYCR, the bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure.

(f) the bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above mentioned conditions.

5.10Small accounts:

'Small account' means a saving account introduced in terms of Government of India, Notification No.14/2010/F.No.6/2/2007–E.S dated 16th December 2010, where:
the aggregate of all credits in a financial year does not exceed Rs. 1,00,000/-;
the aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000/-; and
the balance any point does not exceed Rs.50,000/-.

- Bank will allow to open a small account on production of self-attested photograph and affixation of signature or thumb impression as the case may be, on the Account Opening Form provided that:
- The Branch Official of the Bank [authorized as "Designated Officer" for the purpose of opening of small accounts], while opening the small account will certify under his signature that the person opening the account has affixed his signature or thumb impression, as the case may be, in his presence.
- It will be ensured that no foreign remittances are credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;
- 'Small Accounts' shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months in case such account holder provides evidence to the bank of having applied for any of the 'officially valid documents' within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;
- 'Small Accounts' shall be monitored and if there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through production of 'officially valid documents' and Aadhaar Number or where an Aadhaarnumber has not been assigned to the customer through the production of proof of application towards enrolment for Aadhaar which is not more than six months old, along with an OVD. Provided further that if the customer is not eligible to be enrolled for an Aadhaar number, the identity of the customer shall be established through the production of an OVD.;
- Foreign remittance shall not be allowed to be credited into small accounts unless the identity of the client is fully established through the production of officially valid documents.

5.11Operation of accounts & money mules:

"Money Mules" are used by the criminals to launder the proceeds of fraud schemes e.g. phishing and identity theft who gain illegal access to deposit accounts by recruiting third parties to act as 'Money Mules'. In some cases these third parties may be innocent while in others they may be having complicity with criminals.

In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment websites, social networking sites, instant messaging and advertisements in newspapers. As and when they are caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times, the address and contact details of such mules are found to be fake or not upto date, making it difficult for enforcement agencies to locate the account holder.

Bank will ensure to include the names of the money mules reflecting complicity with the criminals will be included in the Internal Watch List and matter will be reported to FIU-India by way of STR. While the accounts such mule accounts as and when identified, will be closed with the approval of the Incumbent Incharge after giving due notice.

However, in order to avoid hardship to innocent mule account holder, they may be permitted to continue with their existing account or to open another account with the same KYC documents.

5.12Bank no longer knows the true identity:

In the circumstances where the Bank cannot ascertain the true identity of the account holder, the bank will file Suspicious Transaction Report (STR) to FIU India.

5.13Monitoring of transactions:

On-going monitoring is an essential element of effective KYC procedures. The risk can be effectively controlled and reduced by understanding the normal and reasonable activity of the customer and by having means to identify transactions that fall outside the regular pattern of the activity of the customer. The extent of monitoring will depend on the risk sensitivity of the account. Special attention will paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

Bank will develop / deploy a software for the purpose of monitoring AML alerts based on the pre-defined scenarios. These scenarios will be periodically reviewed to make these more effective based on the feedback received and experience gained.

Bank will prescribe threshold limits for all categories of accounts on the basis of the nature of business activity, social and financial status, and volume of turnover and location of the customer.

Monitoring of transactions will broadly involve the following:

- Transactions that involve large amounts of cash inconsistent with customer's normal/expected activity/profile will receive special attention.
- Very high account turnover, inconsistent with the balance maintained, income declared, may indicate the funds are being "washed" through the account.
- Special attention will be paid to all complex, unusually large transactions which have no apparent economic or visible lawful purpose and suspicious patterns that indicate violation of the laws of the country threatening its financial well-being.
- Accounts classified under High Risk will be subjected to more frequent and intensive monitoring based on key indicators taking note of the customers background, country of origin, sources of funds, the type of transactions involved and other risk factors.
- The accounts of bullion dealers (including sub-dealers) and jewelers will be categorized as "High Risk".
- Multi Level Marketing Companies: Transactions in the accounts of MLM will be closely monitored and such accounts will be categorized as "High Risk".

5.14Risk categorization, review &updation:

Bank will categorize each new customer for the purpose of "Risk" assessment, based on identity, social/financial status, nature of business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. Bank to seek only such information from the customer, which is relevant to the risk category and is not intrusive and will ensure that such information is kept confidential and details/information so collected is not divulged for cross selling or any other purposes.

For the purpose of risk categorization, individuals (other than High Net Worth clients) 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 will be categorized as low risk. [Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location/address of the customer are to be met].

Categorize customers that are likely to pose a higher than average risk to the bank will be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Bank will apply enhanced due diligence measures based on the risk assessment, requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

In view of risk involved in cash intensive business, accounts of bullion dealers (including sub-dealers) and jewelers will be categorized as 'high risk' requiring enhanced due diligence.

- Other customers to be categorized as high risk are:
    a. High net worth individuals;
    b. Trusts, charities; NGOs and organizations receiving donations;
    c. Companies having close family shareholding or
    d. Politically Exposed Persons [PEPs] ; customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner,

e. Those with dubious reputation as per public information available etc. However, only NPOs/NGOs promoted by United Nations or its agencies will be classified as low risk customers.

- Bank will periodically review the risk categorization of those accounts which require the need for applying enhanced due diligence measure. Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months or earlier depending upon the transaction and/or change in status of the account. Bank should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary the source of funds.

- The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by banks are extremely important for effective implementation of KYC/AML/CFT measures. Accordingly, bank will complete the process of risk categorization and compiling/updating profiles of all the existing customers in a time bound manner.

- In addition to what has been indicated above, Bank will take steps to identify and assess the ML/TF risk for customers, countries and geographical areas as also for products / services / transactions / delivery channels and will frame policies, controls and procedures with the approval of the board, to effectively manage and mitigate the risk adopting a risk-based approach as per the initiative taken by IBA.

- Bank will adopt enhanced measures as per the indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring; High & Medium Risk: customers/ Products Services/Geographies/ Locations/ Alerts for branches/ departments that should trigger suspicion at the time of processing of customer's transaction and not in line with customer's profile.

5.15Closure of accounts:

Where the bank is unable to apply appropriate KYC measures due to no furnishing of information and/or non-cooperation by the customer, the bank will consider closing the account after issuing due notice, to the customer explaining the reasons for taking such decision. Such decisions shall be taken by the Incumbent Incharge at a sufficiently higher level.

Before taking the final step of closing an account due to non-compliance with KYC/AML requirements, as an initial measure, such accounts may be placed under close watch and non-compliant customers may be deprived of certain additional facilities such as issuance of ATM/Debit Card; providing Internet banking services till the customer complies with such requirements.

This exercise, however, should not extend beyond a period of three months. In case the customer despite such measures, shows unwillingness to comply with KYC/AML/CFT requirements, branches are free to proceed further and close the accounts after giving due notice to him/her.

5.16Risk management – internal control system:

A Senior Officer in a suitable rank will be nominated as Compliance cum- Money Laundering Reporting Officer (CMLRO), who would be responsible for compliance of KYC / AML guidelines.

Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts to the staff members. Senior Officers from the Regional Offices, during their visits to the branches will ensure that monitoring of KYC / AML measures are being strictly adhered to as per the laid down procedures, keeping in view the risk involved in a transaction, account or banking/business relationship.

Independent evaluation of the compliance functions of the Banks' policies and procedures, including legal and regulatory requirements

At the end of every calendar quarter, implementation and compliance of concurrent/ internal audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.

5.17Introduction of technology products – internet banking / debit cards / smart cards / gift cards:

Bank will pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking. The Bank will not provide internet facility/technology product to any person without compliance of KYC guidelines and without customer's specific request/understanding of the product. The bank will ensure that full KYC/AML procedures are duly applied before providing internet facility / issuing debit cards / smart cards / gift cards etc. including on the add-on/supplementary cardholders.

The amount transferred / received through electronic mode, beyond a threshold limit, of Rs. 50,000/- and above would be to the debit of the accounts of the customers concerned.

The agents, if any, engaged or appointed for the purpose of marketing of any product including debit cards / smart cards / gift cards etc., would also be subjected to full KYC measure.

5.18Combating financing of terrorism:

The Bank will ensure before opening the account that the name(s) of the proposed customer does not appear in the lists of designated/banned individuals / entities circulated by RBI/Bank from time to time.

Bank will ensure to update the following list of individuals and entities for the purpose of scanning the names of the individuals before opening of accounts:

- "'ISIL (Da'esh) & Al-Qaida Sanctions List" is maintained by 1267 / 1989 Committee with respect of those individuals, groups, undertakings and other entities associated with ISIL (Da'esh) & Al-Qaida; and
- "1988 Sanctions List" is maintained by 1988 Committee and consists of names of those individuals, groups, undertakings and other entities associated to Taliban.

- Bank to note that “ISIL (Da'esh) & Al-Qaida Sanctions List” and “1988 Sanctions List” are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.
- Bank will also scan all the existing accounts to ensure that no account held is linked to any of the individuals/entities in the list. In case the full details of accounts bearing resemblance with any of the individuals/entities in the list, the branch will report to the Head Office for submitting report to RBI and FIU-India.
- The Bank will take into account risks arising from deficiencies in Anti-Money Laundering/Combating of Financing of Terrorism regime of certain jurisdictions as identified by Financial Action Task Force (FATF) at their website and informed through RBI/Bank from time to time.
- The Bank will develop suitable mechanism for enhanced monitoring of transactions suspected of having terrorist links and swift identification of transaction and submitting suitable reports to the FIU-India on priority.

5.19Freezing of assets under section 51A of unlawful activities, (prevention) act, 1967-prevention of and coping with terrorist activities.

- The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by Unlawful Activities (Prevention) Amendment Act, 2008. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or listed entities, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or Listed entities or any other person engaged in or suspected to be engaged in terrorism.

- Bank will strictly follow the procedure laid down in the Government of India, Ministry of Home Affairs, Internal Security-I Division, New Delhi Order No.17015/10/2002-IS-VI dated 27th August, 2009

5.20Wire transfer

5.20.1 Cross border wire transfer

FINO Payment bank shall ensure the following in cross border wire transfer:

i) All cross-border wire transfers will be accompanied by accurate and meaningful originator information.

ii) Information accompanying cross-border wire transfers will 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, will 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.

iv) As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Bank shall ensure to refer to such list and prohibit dealing with such individuals, groups and entities.

v) Additionally the bank shall also refer to the World-Check database of Politically Exposed Persons (PEPs) and heightened risk individuals and organisations to identify and manage financial, regulatory and reputational risk.

vi) FEMA regulations need to be complied for both Inward and Outward transfer, details of which will be mentioned in the Remittance Policy of the Bank.

5.20.2 Domestic wire transfers

i)Information accompanying all domestic wire transfers of Rs.50,000/- and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

ii) If a bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs.50,000/- to several beneficiaries in order to avoid reporting or monitoring, the bank 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 made to FIU-IND.

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

iv) However, this would not apply to Interbank transfers and settlements where both the originator and beneficiary are banks / Financial Institutions.

5.21 Role of Ordering, Intermediary and Beneficiary banks

5.21.1 Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

5.21.2 Intermediary Bank

Bank, if processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

5.21.3 Beneficiary Bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are

suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

5.22Principal Officer (PO)

- Bank will designate a senior management officer as Principal Officer, who will supervise and monitor all the activities in respect of KYC/AML/CFT measures.
- Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. Principal Officer will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.
- The Principal Officer will also be responsible for timely submission of CTRs/STRs/CCRs/NTRs to FIU-India.
- For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data and other Customer Due Diligence information, transaction records and other relevant information.

5.23Maintenance and Preservation of Records

5.23.1 Maintenance of records of transactions

In terms of Section 12 of the Prevention of Money Laundering Act, 2002, Bank will preserve and maintain proper record of all transactions including the records as mentioned below in terms of Prevention of Money Laundering (Maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing information and verification and maintenance of the Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (came into operation with effect from12.02.2010)a. All cash transactions of the value of more than Rupees Ten lakh or its equivalent in foreign currency;

b. All series of cash transactions integrally connected to each other which have been valued below Rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- need not be reported in the Cash Transaction Report.

c. All transactions involving receipts by non-profit organizations of value more than Rupees ten lakh or its equivalent in foreign currency.

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

e. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

5.23.2 Record/Information to be preserved

Bank will maintain all necessary information in respect of transactions referred in (a). to (e) above in 5.20 (i) to permit reconstruction of individual transaction, including the following information:

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

5.23.3 Maintenance and Preservation of record

a. Bank will maintain the records containing information of all transactions including records of transactions mentioned in 13 (a. to e) above. Further, bank will maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic and international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.
b. The records pertaining to the identification of the customer and his
address (e.g. copies of documents like passports, Identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, will be properly preserved for at least five years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.
c. Special attention will be paid to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Further, the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to auditors in their day-to-day work relating to scrutiny of transactions and also to RBI/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

5.24CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

Fino will capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for ‘individual’ and ‘Legal Entities’ as the case may be.

Accordingly, Fino will take the following steps:

- In the first phase, Fino will upload the KYC data with CERSAI, in respect of new individual accounts opened on or after July 15, 2016
- Operational Guidelines (version 1.1) for uploading the KYC data has been released by CERSAI. Further, ‘Test Environment’ has also been made available by CERSAI for the use of by Banks. Fino will utilise the same.

5.25Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, Fino shall determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- Register on the related e-filling portal of Income Tax Department as a Reporting Financial Institutions
- Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

  Explanation: Fino shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/ RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.
- Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

5.26Reporting to Financial Intelligence Unit-India

In terms of Prevention Money Laundering Act 2002 and as amended by Prevention Money Laundering (Amendment) Act 2009, Bank will ensure to submit the following reports to Financial Intelligence Unit-India.

FIU-India has developed a utility i.e. fin NET Project and now Suspicious Transaction Reports (STRs), Counterfeit Currency Reports (CCRs) and Cash Transaction Reports (CTRs) are submitted to them online.

5.26.1 Cash Transaction Report (CTR)

- Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.
- The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.
- A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through MIS Report: Misc Reports Module under SENSRPT – 5/7 & 5/7a) for production to auditors/Inspectors, when asked for.

5.26.2 Suspicious Transaction Report (STR)

• While determining suspicious transactions, bank will be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time. Suspicious transaction means a transaction, comprising of deposit, withdrawal, transfer of funds, whether or not made in cash which, to a person acting in good faith:

i. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences laid down under PMLA, 2002, an offence regardless of the value involved; or
ii. appears to be made in circumstances of unusual or unjustified complexity; or
iii. appears to have no economic rationale or bonafide purpose; or
iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism, which includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist act or by a terrorist, terrorist organizations or those who finance or are attempting to financing of terrorism; or

- In some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. Banks will report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

- The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions.

- Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction whether cash or non-cash, series of transactions integrally connected are of suspicious nature.

- Bank will ensure not to put any restrictions on operations in the accounts where Suspicious Transaction Report has been made. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.

5.26.3 Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format not later than 15th of the succeeding month from the occurrence of such transactions.

5.26.4 Non Profit Organizations Transaction report [NTR]

Bank will report all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

("Non-Profit Organisation" means any entity or organization i.e. registered as a trust or a society under the Societies Registration Act 1860 or any similar State Legislation or a company registered under Section 25 of the Companies Act, 1956)

5.27Selling Third Party Products

Banks acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

- the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.
- transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

5.28Customer education/ employee training/ hiring of employees

5.28.1 Customer Education

Implementation of KYC procedures would require certain additional information from the customers which may be of personal nature and may not have been called earlier. This may sometime be questioned by the Customer as to the motive & purpose of collecting such information. Bank will, in order to educate the customers about the objective of KYC norms will prepare specific literature/pamphlet to educate the customers about the need of KYC requirement and the information/documents required for making their existing accounts KYC compliant.

5.28.2 Training of Employees

Bank will ensure to have ongoing employee training programmes/seminar in order to sensitize the field staff about KYC/AML/CFT procedures/ modalities/guidelines and changes from time to time. Human resources department of the Bank will ensure to put in place an appropriate training programme on the same in association with compliance department.

5.28.3 Hiring of Employees

In order to ensure that the criminals do not misuse banking channel, it would be ensured that adequate screening mechanism is put in place so that the right type of persons are recruited/hired.

5.29Annexure I

Fino Payment Bank shall refer to the attached template to capture the KYC Information of the bank's customers for sharing the same with the Central KYC Records Registry (CKYCR)

5.30Annexure II

The level of Money Laundering (ML) risks that the Bank is exposed to by a Customer relationship depends on:

- Type of the customer and nature of business
- Type of product / service availed by the customer
- Country where the Customer is domiciled.

Based on the above criteria, FINO Payment bank shall classify customers into three Money laundering Risk levels.

Customers will be classified in the following risk categories-

(i) High Risk

a) who are engaged in certain professions where money laundering possibilities are high. Eg. Antique Dealers (individuals and entities), Money Services Bureau (entities - not employees of these entities) and dealers in arms

b) who live in “high risk countries” (nationality is irrelevant).

c) Politically Exposed Persons (PEPs) – The Bank may obtain additional information disclosing the source of funds that would be deposited in the account.

Opening of the above accounts would need specific approval of senior personnel (as can be decided by each bank).

(ii) Medium Risk

Customers are classified as Medium if they/any of the account holders live(s) in a Medium risk country.

Non-individual current account customers excluding proprietorship concerns (Individual)will be classified as medium risks. The risk classification may be lower for those customers where there is sufficient knowledge in the public domain available to the bank (e.g. listed companies, regulated entities, etc)

(iii) Low Risk

All customers that are not High/Medium Risk are Low Risk customers. (additionally bank shall at its discretion classify customers as low risk for a specific type and category of customers based on the extent of knowledge/information available on such customers to prove their identity sufficiently.

Indicative list High Risk Countries
Country
Myanmar (Burma)
Nigeria
Turkmenistan
Ukraine
Guatemala
Cook Islands
St Vincent & the Grenadines
Russia

Angola
Zimbabwe
Afghanistan
Cuba
Iraq
Libya
Azerbaijan
Moldova
Kazakhstan
Georgia
Uzbekistan
Belarus
Armenia
Kyrgyzstan
Tajikistan
Cook Islands

Medium Risk Countries
- All countries in Africa
- All countries in the Americas other than USA and Canada

An Indicative List of Suspicious Activities Transactions Involving Large Amounts of Cash
(i) Exchanging an unusually large amount of small denomination notes for those of higher denomination;
(ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
(iii) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
(iv) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
(v) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;
(vi) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

6.Glossary

This section contains the definition of key terms used in the policy as per the applicable regulatory guidelines and industry standards.

Regulatory reference

The following key regulation is applicable to the current policy document.

Regulator	Regulation name	Regulation date	Regulation code
RBI	Master Direction – Know Your Customer (KYC) Direction, 2016	Feb 25th, 2016(Updated April 20,2018)	RBI/DBR/2015-16/18 DBR.AML.BC.No.81/14.01.001/2015-16

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PML Act	Prevention of Money Laundering Act
CDD	Customer Due Diligence
FATF	Financial Action Task Force
CFT	Combating Financing of Terrorism
NOC	No Objection Certificate
PEP	Politically Exposed Person
POA	Power of Attorney
KYC	Know Your Customer
AML	Anti-Money Laundering