FYNX CAPITAL LIMITED
(formerly known as Rajath Finance Limited)

Policy Guidelines on 'Know Your Customer' norms and Anti-Money Laundering measures

Table of Contents

Introduction

Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for Non-Banking Finance Companies (NBFCs) thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers vide Circular Nos.: DNBS (PD) CC No. 34/10.01/2003-04, dated 06-01-2004, DNBS (PD) CC No. 48/10.42/2004-05, dated 21-02-2005, DNBS (PD) CC No. 64/03.10.042/2005-06, dated 07-03-2006. The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this code to conform to the standards so prescribed. This policy is applicable across all branches / business segments of the Company, and its financial subsidiaries and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which shall be advised by RBI from time to time.

Similarly, KYC guidelines have been issued by NSDL and CDSL on customer identification and proof of address at the time of opening the account and for subsequent changes/modification etc. Detailed master circulars have been issued by NSDL and CDSL based on the SEBI guidelines from time to time on the account opening, nomination, changes/modification/closure, operations, audit etc. in respect of different types of customers.

The Company endeavors to frame a proper policy framework on 'Know Your Customer' (KYC) and Anti-Money Laundering measures. The Company is committed for transparency and fairness in dealing with all stakeholders and in ensuring adherence to alt laws and regulations. The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof for cross selling or any other purposes. The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconsistent with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his /her consent and after effective rendering of services.

The Company shall also communicate its KYC norms to its customers. The Company shall ensure that the implementation of the KYC norms is the responsibility of the entire organisation.

The Company's Board of Directors and the management team are responsible for implementing the KYC norms hereinafter detailed, and also to ensure that its operations reflect its initiatives to prevent money laundering activities.

For the purpose of KYC policy, a 'Customer' shall be defined as:

- A person or entity that maintains and/or has a business relationship with the Company;
- One on whose behalf such relationship 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 reputation or other risks to the Company, say, a wire transfer or issue of a high value demand draft as a single transaction.

Objective:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The Company hereunder framing its KYC policies incorporating the following four key elements:

- Customer Acceptance Policy
- Customer Identification Procedures;
- Monitoring of Transactions; and
- Risk management.

Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) for the Company are given below:

- No account is opened in anonymous or fictitious/ benami name(s).
- The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category.
- Accept customers after verifying their identity as laid down in customer identification procedures.
- While carrying out due diligence the Company shall ensure that the procedure adopted shall not result in denial of services to the genuine customers.
- For the purpose of risk categorisation of customers, the Company shall obtain the relevant information from the customer at the time of account opening.
- Parameters of risk perception shall be clearly defined in terms of the 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 low, medium and high risk; customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs – as explained in Annex II) may, if considered necessary, be categorized even higher;

- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering (PML) Act, 2002 and guidelines issued by Reserve Bank from time to time;
- The Company shall not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It shall be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking as there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity and
- Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
- The Company shall prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the Company. However, while preparing the customer profile the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
- For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk. Illustrative examples of low-risk customers would 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 & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher-than-average risk to the bank may be categorized as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

- Examples of customers requiring higher due diligence may include
- non-resident customers,
- high net worth individuals,
- trusts, charities, NGOs and organizations receiving donations,
- companies having close family shareholding or beneficial ownership,
- firms with 'sleeping partners',
- politically exposed persons (PEPs) of foreign origin,
- non-face to face customers, and
- those with dubious reputation as per public information available, etc.
- Adoption of customer acceptance policy and its implementation shall not become too restrictive and shall not result in denial of financial services to the general public, especially to those, who are financially or socially disadvantaged.
- As advised by RBI under Circular No. DNBS(PD)CC.No.193/03.10.42/2010-11, the Company shall not allow opening and/or holding of an account on behalf of a client/s by professional

intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

Customer Identification Procedure (CIP)

The policy clearly spells out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the business relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such a risk-based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). For customers that are natural persons, the Company shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall

- verify the legal status of the legal person / entity through proper and relevant documents
- verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person,
- Understand the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person. The Company shall take into account Customer identification requirements in respect of a few typical cases, especially; legal persons requiring an extra element of caution are given in Annexure-II as per Circular No.: DNDS (PD) CC NO. 48/10.42/2004-05 dated 21-02-2005 for guidance of NBFCs. The Company shall frame its own internal guidelines based on their experience of dealing with such persons/entities, normal lenders prudence and the legal requirements as per established practices. The Company shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.
- An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the Annexure-I.

The documents requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

Customer Identification Procedure is to be carried out at different stages i.e.

- While establishing a business relationship (or)
- Carrying out a financial transaction (or)
- Where the Company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any.

- When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

No deviations or exemptions shall normally be permitted in the documents specified for account opening. In case of any extreme cases of exceptions, concurrence of Policy Head shall be obtained duly recording the reasons for the same. Suitable operating guidelines for implementation of the KYC/ AML guidelines shall be issued by the Company for its different business segments from time to time.

Allotment of Unique Customer Identification Code (UCIC)

As required by the RBI guidelines DNBS/ PD.CC.No.325/03.10.42/2012-13 dated May 3, 2013, the Company shall allot Unique Customer Identification Code to all its new customers while entering new relationships. Further for the existing customers such a code would be created within the permitted timeframes. This UCIC will be used to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable NBFCs to have a better approach to risk profiling of customers.

Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits, Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. The Company does not accept any deposits. Further, there are no operative accounts where the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary. Most of the Company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the Company are purely shall be restricted to the EMI/loan repayable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI/loan payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions whatsoever nature other than repayment of loan with interest is carried out by the customer with the Company.

As per RBI Circular No. RBI/2010-11/419 DNBS (PD) CC No 212/03.10.42/2010-11 NBFCs were further advised that in view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) and jewelers should also be categorized by NBFCs as 'high risk' requiring enhanced due diligence. The Company shall implement the same and classify such bullion dealers and jewelers under "high risk" category and any transactions in their loan accounts would be monitored on a daily basis.

The permanent correct address shall mean 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 Company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative: wife, son, daughter and parents etc. who live with their husband, father/mother and son, the Company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The Company shall use any supplementary evidence such as a

letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, the Company shall keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. The Company shall ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority.

The Company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation shall not be less than once in five years in case of low-risk category customers and not less than once in two years in case of high and medium risk categories

The Company shall ensure that its branches continue to maintain a proper record of all cash transactions. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to the controlling / head office on a fortnightly basis.

Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the “offence of money laundering” as under:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering”.

The Company shall adopt the guidelines issued by RBI for Prevention of Money Laundering vide Circular No. DNBS (PD) CC No. 48/10.42/2004-05 dated 21-02-2005.

For assessment and monitoring of the risk categorization of the customers, the Company would take into consideration to necessary extent, the Guidance note on KYC norms / AML Standards issued by Indian Banks Association (IBA) for Banks as advised by RBI vide its Circular No. RBI/2011-12/466 DNBS(PD).CC. No 264/03.10.42/2011-12 dated March 21, 2012.

All transactions of cash and suspicious as required under PML Act 2002 shall be reported to FIU from time to time. The Principal Officer specified by the Company shall ensure that such a reporting system is in place and shall monitor receipt of the reports. The name of the Principal Officer shall be specified by the CEO of the Company from time to time.

All transactions of suspicious nature and / or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority by the Principal Officer.

Maintenance of records of transactions

The Company shall introduce a system of maintaining proper record of transactions prescribed under rule 3, as mentioned below:

- all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- 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 transactions exceeds rupees ten lakh;
- 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;

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

Preservation of records

The Company shall maintain the following information in respect of transactions referred to in rule 3:

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

The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, the Company shall maintain for at least ten years from the date of cessation of transaction between the Company and the client, all necessary records of transactions, both domestic or international, which shall 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.

The Company shall ensure that 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, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data shall be made available to the competent authorities upon request.

Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, the Company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND). The Company shall adopt the format prescribed; follow timelines, guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. The Company shall initiate urgent steps to ensure electronic filing of cash transaction reports (CTR). The Company shall not put any restrictions on operations in the accounts where an STR has been made. However, it shall be ensured that there is no tipping off to the customer at any level.

For determining integrally connected cash transactions, NBFCs shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month.

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The Company shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. The Company shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

The Company shall make STRs if they have reasonable grounds to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the Company shall consider the indicative list of suspicious activities contained in Annex-III

Risk Management

The Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship. The Company's internal audit and compliance functions shall have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function shall provide independent evaluation of the Company's own policies and procedures including legal and regulatory requirements. The Company shall ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent / Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals.

The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

Customer Education

Implementation of KYC procedures requires the Company to demand certain information from customers which shall be of personal nature or which have hitherto never been called for. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company shall prepare specific literature/pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with customers.

Introduction of New Technologies - Credit cards

The Company shall pay special attention to any money laundering threats that shall arise from new or developing technologies including internet transactions that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many Companies are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Further, marketing of these cards is generally done through the services of agents. The Company shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers, if any, in future; agents shall also be subjected to KYC measures.

Accounts of Politically Exposed Persons: Customer Due Diligence (CDD) measures shall be made applicable to Politically Exposed Person (PEP) and their family members or close relatives. In the event

of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Combating financing of terrorism

- In terms of PMLA Rules, suspicious transactions shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and

  swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

- As and when the list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the Company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities shall be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. The Company shall before opening any new account, ensure that the name/s of the proposed customer does not appear in the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the Company as an integral part of recruitment/hiring process of personnel.

The Company shall take into account risks arising from the deficiencies in AML/CFT regime of countries of Iran, Angola, Democratic People's Republic of Korea (DPRK), Ecuador, Ethiopia, Pakistan, Turkmenistan and Sao Tome and Principe and list of countries circulated by RBI from time to time.
In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the Company shall consider the indicative list of suspicious activities contained in Annex- III

Applicability to branches and subsidiaries outside India (Presently we do not have any branches outside India, shall be applicable whenever branches are opened outside India)

The extant instructions that KYC/AML guidelines issued by Reserve Bank of India shall also apply to their branches and majority owned subsidiaries located outside India, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. It is further clarified that in case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of the Company shall adopt the more stringent regulation of the two.

Appointment of Compliance/Principal Officer

The Company has a senior management officer to be designated as Compliance/Principal Officer. Compliance/Principal Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He shall 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. The Manager appointed under Companies Act shall be the Compliance/ Principal Officer of the Company for this purpose.

The Company shall abide by all guidelines, directives, instructions and advice of Reserve Bank of India as shall be in force from time to time. The contents in this document shall be read in conjunction with these guidelines, directives, instructions and advice. The Company shall apply better practice so long as such practice does not conflict with or violate Reserve Bank of India regulations.
Demat Accounts:

The Company shall follow all the guidelines issued by NSDL/CDSL and SEBI from time to time in respect of opening, capturing the details in the DPM system and maintenance of demat accounts. Necessary documents as prescribed by them for Proof of Identity (POI) and Proof of Address would be obtained at the time of opening the account. The procedures for in person verification would also be ensured as detailed out in the master circulars. The compliance with the guidelines would also be subjected to audit as prescribed in the master circulars. These guidelines would stand auto corrected in tandem with any subsequent clarification / modification in the guidelines issued by NSDL and CDSL based on SEBI directives. Necessary scrutiny of the transactions based on the reports / dumps received from NSDL/CDSL or suo moto would be made for identifying and reporting suspicious transactions, if any.

The Company shall adhere to the KRA requirements referred in SEBI Circular MIRSD/CIR-26/2011 dated December 23, 2011. KYC Registration agency (KRA) has been registered with SEBI under the Securities and Exchange Board of India (KYC (Know Your Client) Registration Agency) Regulations 2011. CDSL Ventures Limited, a wholly owned subsidiary of CDSL is a registered KRA. The Company being an intermediary would get registered with CVL KRA. The Company would follow strictly all the KRA operating instructions and comply with all the requirements. All the clients existing and prospective would be made aware of the requirements of the KRA in ensuring proper KYC compliance with effective date January 1, 2012.
This document is the property of the Company. It contains information that is internal to the Company and is of competitive value and sensitive in nature. All employees must treat its contents as confidential and keep it secure.

Annexure — I

Customer Identification Procedure Features to be verified and documents that shall be obtained from customers

KYC CHECKLIST	
Features to be verified and documents that shall be obtained from customers	
Features	**Documents**
Identity Proof (Individual)	Passport
	Photo PAN card
	Voter's Identity Card / UID Aadhar Card
	Laminated Driving license - Permanent. For a Driving license coming in a booklet form (Not laminated) to be acceptable as a KYC document, an OSV done by an RCL employee on the photocopy of the Driving license would be mandatory.

	Employee ID card (MNCs / PSUs / Public Limited Companies/Other Government companies and not Pvt. Ltd. Co)
	Photo Ration Card
	Photo Debit Card
	Bankers' verification/passbook with stamp on photograph along with applicant's signature. This can be accepted provided it contains the customer's photo and signature, a/c number, date of opening, branch name, address and it shall be certified only by the Branch Manager or Operations Head with their name & designation.
	Defence ID Card
	Photo credit Card - provided the card is valid & current and is at least 3 months old
Address Proof (Individual)	Telephone Bill
	Life Insurance Premium receipt of any insurer (Policy shall be minimum 12 months in force)
	Post paid Piped gas connection bill showing consumption and full address
	Electricity Bill
	Ration Card
	Voter's Identity Card
	Laminated Driving license - Permanent. For a Driving license coming in a booklet form (Not laminated) to be acceptable as KYC document, an OSV done by RCL employee on the photocopy of the Driving license would be mandatory.

	Passport
	Copy of sale agreement if current residence is owned
	Cooperative Housing society Receipt to be taken provided residence FI is positive at the same address
	Leave & License agreement if the applicant is staying on rent & the agreement is registered / notarized. Wherever notarized Leave & License agreement is taken, the notarization shall be in original & the agreement shall be executed on a stamp paper as per the respective State Stamp Act(mail already circulated to all in the past on the same) Applicable to lease deed also.
	Postpaid Mobile Bills
	Bank Passbook/ Latest Bank Account Statement (first page of the same with full address mentioned which matches with the applicant's address as per the Application form). In case of a Bank Passbook, the page showing the latest banking transaction shall be taken on record.
	Front Copy of the Credit Card and latest Card statement
	Municipality Water Bill
	Municipal tax receipt/ Property tax receipt
	Office Identity card mentioning the address (MNCs/PSUs/Public Limited Companies/Other Government companies) OR letter from employer if the applicant stays in the Company provided accommodation)
	All utility bills and credit card statements shall be less than 3 months old

Signature verification (Individual)	Margin Money Cheque Clearance if paid favoring RCL (Copy of cheque taken prior to clearing)
	Passport
	Laminated Driving license - Permanent. For a Driving license coming in a booklet form (Not laminated) to be acceptable as KYC document, an OSV done by RCL employee on the photocopy of the Driving license would be mandatory.
	PAN Card
	Bankers Verification
	Photo Debit Card with scanned signatures
	Copy of entire Registered Sale deed showing Photo & signature
	Photo credit Card with scanned signatures - provided the card is valid & current and is at least 3 months old
	Government ID card for govt. employees
KYC Docs for Entities (Self Proprietorship / Partnership / Companies)	

a) Proof of Legal Existence and Registered Office Address	For Partnership firms, Partnership Deed or Certificate of Registration from Registrar of firms in case the firm is registered
	For Companies, MOA & AOA along with Certificate of Incorporation. In case of Public Limited Company, Certificate of Commencement of Business also to be taken.
	PAN Card of partnership firms or companies can be taken as proof of existence. (In this case separate proof of registered address needs to be taken)
	Sales tax registration Certificate
	Shop & Establishment Certificate
	Factory Registration Certificate
	SSI Registration Certificate
	Importer - Exporter Code Certificate
	VAT / Service Tax Registration Certificate.
	Latest Bank Account Statement in the name of the Entity with full address mentioned which matches with the entity's address as per the Application form along with Banker's Verification of the Authorized Signatory of the entity

b) Proof of Operating Address	Telephone Bill / Electricity Bill in the name of the entity
	Leave & License agreement in the name of the entity if the entity is operating its business from a rented premises & the agreement is registered / notarized. Wherever notarized Leave & License agreement is taken, the notarization shall be in original & the agreement shall be executed on a stamp paper as per the respective State Stamp Act (mail already circulated to all in the past on the same)
	IT Assessment Order
	Pan Intimation letter
	Acknowledged ITR of the entity
	Latest Bank Account Statement in the name of the Entity with full address mentioned which matches with the entity's address as per the Application form along with Banker's Verification of the Authorized Signatory of the entity
	In case of Self Proprietorship concerns, proof of the operating address could be taken in the individual's name as long as the Office FI is positive at the address from where the individual is operating his business. This shall match with the office address given by the individual as per the Application form. Office FI in this case shall not be negative on account of applicant not running business from the same premises.
c) Trust/Society	Certificate of registration, if registered
	Trust Deed/ Constitutional Documents of the trust / Society
d) Signature verification	ECS mandate with the signatures of authorized signatories and with the stamp

of the Authorized Signatory of the Entity	of entity - Verified and acknowledged by the banker pre-disbursement.
	Clearance of Initial payment cheque equal to an amount of the EMI and confirmed by local ops

	Certain companies have GPAs for signing PDCs. The GPA can be an SV subject to the GPA carrying the signature of the auth signatories along with their names & certified only by the Branch Manager or Operations Head with their name & designation. Care must be taken to verify the GPA for any specific covenants such as (a) If GPA is applicable for a particular bank account, and then PDCs must be from the same bank account (b) Whether GPA is valid indefinitely or has an expiry date. In a case where there is an expiry date then the validity of GPA shall be > contract tenure otherwise such GPA becomes invalid
	Documents which would have been submitted to the banker at time of opening of account by the entity stating the authorised signatories of the bank account. These documents again shall be certified by the Branch Manager or Operations Head with their name & designation
	Bankers Verification of the Entity's Authorised Signatory from where the PDCs are issued.
Proprietary Concerns (Care: As per Circular No. RBI/2011-12/579 DNBS (PD).CC. No 275 /03.10.42 /2011-12 dated May 29, 2012 any two of the documents listed should be obtained for identity of the proprietory concern. These documents should be in the name of the proprietory concern.)	i) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence 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, Licence 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, etc
	ii) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. NBFCs/RNBCs may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.
	iii) 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.
	iv) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.
	Two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Annexure - II

Customer Identification Requirements – Indicative Guidelines Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks shall determine whether the customer is acting on behalf of

another person as trustee/nominee or any other intermediary. If so, banks may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

Banks need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with banks. Banks shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a 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 shall not be necessary to identify all the shareholders.

Client accounts opened by professional intermediaries

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are commingled at the bank, the bank shall still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they shall satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It shall be understood that the ultimate responsibility for knowing the customer lies with the bank.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public 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. Banks shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP shall be taken at a senior level which shall be clearly spelt out in Customer Acceptance policy. Banks shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

Beneficial Ownership

As per Rule 9(IA) of the Prevention of Money Laundering Rules, 2005 the Company shall identify the beneficial owner and take all reasonable steps to verify his identity.
Beneficial Ownership has been defined in RBI Circular No. RBI/2012-13/422 DNBS (PD).CC. No 321 /03.10.42 /2012-13 dated February 27, 2013 as given below.

The term ';beneficial owner'; has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person. The Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:

- Where the client is a person other than an individual or trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:
- The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

  Explanation: Controlling ownership interest means ownership of/entitlement to more than 25 percent of shares or capital or profits of the juridical person, where the juridical person is a company; ownership of/entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or, ownership of/entitlement to more than 15% of the property or capital or profits of the juridical person where the juridical person is an unincorporated association or body of individuals.

- In cases where there exists doubt under (i) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

  Explanation: Control through other means can be exercised through voting rights, agreement, arrangements, etc.

- Where no natural person is identified under (i) or (ii) above, the identity of the relevant natural person who holds the position of senior managing official.
- Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Annex -III

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash
Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the Company, e.g. cheques,
Transactions that do not make Economic Sense
Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer furnishes a plausible reason for immediate withdrawal.
Activities not consistent with the Customer's Business

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

Attempts to avoid Reporting/Record-keeping Requirements

- A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.
- An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

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

Customer who provides Insufficient or Suspicious Information

- A customer/Company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
- A customer/Company who is reluctant to reveal details about its activities or to provide financial statements.
- A customer who has no record of past or present employment but makes frequent large transactions.

Certain NBFC Employees arousing Suspicion

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