Davinta Financial Services Pvt. Ltd.
7-P, 93-P, Electronic City West, Bangalore-560100, India
Tel: 080-4905 4444 / 3350 4444

Davinta
Manzil Aapki Raah Humari

DAVINTA FINANCIAL SERVICES PRIVATE LIMITED

POLICY FRAMEWORK ON "KNOW YOUR CUSTOMER (KYC) AND "ANTI-MONEY LAUNDERING MEASURES"(AML)

1. INRODUCTION

Davinta Financial Services Private Limited hereinafter referred to as "Company" or "Davinta", recognizes its role as a corporate entity and endeavors to adopt the best practices with the highest standards of governance through transparency in business ethics, accountability to its customers, government and others. This Anti–Money Laundering (AML) and Know your customer (KYC) policy is thus being designed as per "Master Direction DBR.AML.BC.No.81/14.01.001/2015-16" and the guidelines mentioned therein, as amended from time to time. Davinta is committed to the highest standards of AML, Counter Terrorism Financing (CFT), Anti –Fraud and other punishable criminal acts.

The Board of Directors, Management and all employees shall adhere to these standards to protect the Company and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

Davinta ensures compliance with the RBI Master Direction on KYC by aligning its KYC policy with the established guidelines. Our KYC policy, tailored to our lending, credit operations, and financial dealings, encompasses with the four key elements:

(i) Customer Acceptance Policy;
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions; and
(iv) Risk management.

2. DEFINITIONS

- **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

- **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

- **"Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to

receive, store, safeguard and retrieve the KYC records in digital form of a customer.

- **"Customer"** means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

- "**Customer Due Diligence (CDD)** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification."

- "**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 Davinta as per the provisions contained in the Act.

- **"Designated Director"** means a person designated by Davinta to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

- **"Principal Officer"** means an officer at the management level nominated by Davinta, responsible for furnishing information as per rule 8 of the Rules.

- **"Sleeping Partners"** means a partner who takes no share in the active business of a company or partnership, but is entitled to a share of the profits, and subject to a share in losses.

3. OBJECTIVES

- To prevent the Company from being used, intentionally or un-intentionally, by criminal elements for money laundering activities.
- To know/understand the Customers and their financial dealings better, which in turn, help in managing their risks prudently.
- To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. This KYC Policy is applicable to the Company and is to be amended from time to time based on the applicable provisions in the RBI Master Direction.

- To have a proper Customer Due Diligence (CDD) process before onboarding a client.

4. CUSTOMER ACCEPTANCE POLICY (CAP)

Explicit criteria for acceptance of customers

- No account will be opened in anonymous or fictitious / benami name(s)
- Parameters of risk perception are defined in Annexure-3 of this policy.
- Customers are categorized into different level of risk perception as in Section 5 of this policy
- Documentation requirements and other information to be collected in respect of different categories of customers depending upon the perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002.
- Davinta will not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures, i.e. unable to verify the identity and /or obtain documents required as per the risk categorization due to non–co-operation of the customer or non-reliability of the data/information furnished to the Company.
- No transaction or account-based relationship will be undertaken without following the CDD procedure.
- The Company will undertake verification of all documents as per prescribed rules and regulations. However, care will be taken that the implementation of the policy does not lead to harassment of the customer.
- Davinta ensures that the circumstances in which a customer is authorized to act on behalf of another person/entity are clearly outlined in the relevant documentation. These provisions adhere to established laws and practices, ensuring clarity and compliance for all parties involved.
- Cross Checks will be made to confirm 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.
- Where Permanent Account Number (PAN) is obtained, the same will be verified from the verification facility of the issuing authority.

- Where Goods and Services Tax (GST) details are available, the GST number will be verified from the search/verification facility of the issuing authority.
- This customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
- Davinta shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of Davinta desires to open another account or avail any other product or service from it, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

Where Davinta forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file a Suspicious Transaction Report (STR) with FIU-IND.

5. CUSTOMER IDENTIFICATION PROCEDURE

Customer Identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Company will obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship.

Customer Identification Procedure will be carried out at different stages as follows:

A. While establishing a relationship

- Transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transaction that appear to be connected *(As per RBI KYC Master Circular)*, or
- Any international money transfer operations
- Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand

B. When the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data, company

may further demand data as follows:

- For customers that are natural persons, 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 legal status of the legal person/entity to be verified through proper and relevantdocuments. For any person purporting to act on behalf of the legal person/entity, it has to be verified whether he is so authorized and his identification has to be verified. Also, the ownership and control structure of the customer should be understood so as to determine who the natural persons are, who ultimately control the legal person and are its beneficial owners
- For a customer who is intentionally structuring a transaction into a series of transactions below the threshold of Rupees Fifty Thousand.
- An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure – 1.**

6. CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD)" is an essential component of the Customer Identification Procedure. It involves identifying and verifying the customer and the Beneficial Owner using 'Officially Valid Documents' or 'Identification information as mentioned under the RBI's Guidelines, as a 'proof of identity' and a 'proof of address'. This is done in accordance with the manner outlined in this Policy and as prescribed under the RBI's Guidelines on "Know Your Customer" and Anti-Money Laundering Measures, subject to amendments from time to time.

Davinta ensures to capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. **Annexure-1** states about the documents and details required for the Customer Due Diligence.

Further, Davinta has a Board approved policy which outlines a robust due diligence process for managing requests to change the mobile number associated with the accounts of the Customers. Through this process, Davinta tries to mitigate the risk and ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer which they have provided/ shared with Davinta

Below are the methods based on which Davinta onboard the Customer after performing the requisite due diligence.

- **CDD through Video based Customer Identification Process (V-CIP)-** Davinta implements Video-based Customer Identification Process (V-CIP) for seamless verification, adhering to RBI's KYC guidelines. V-CIP involves real-time audio-visual interaction, ensuring secure storage of data in India and compliance with relevant regulations.

- **CDD through Digital KYC-** Davinta conducts Digital KYC for Customer Due Diligence (CDD), capturing live photos and valid identity documents, including Aadhaar where offline verification is not feasible.

Davinta also consider the Enhanced Due diligence measures for non-face-to-face customer onboarding apart from the methods mentioned above. It is required when a customer is perceived to be at a higher risk to the company. A high-risk situation also occurs where there is an increased opportunity for money laundering or terrorist financing through the service or product you are providing. Examples of higher risk customers may include politically exposed people, customers with suspicion of terrorist activities, non-face to face account opening and customers located in high-risk locations. The measures take in case of Enhanced Due Diligence mentioned in **Annexure-2**.

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR): For the purpose of compliance of the provision of Rule 9(1A) of PML Rules as amended from time to time, Company capture customer's KYC information for sharing with the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) platform as authorised by Government of India vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015 and shall act as Central KYC Records Registry (CKYCR). The Company upload the customer's KYC records on CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Once the KYC identifier is generated by CKYCR, the company shall communicate the same to the individual/Legal Entity as the case may be.

Company must incrementally upload or update KYC data for individual/ Legal Entity accounts opened prior to the stipulated dates during periodic updates as per Section 7 of this policy, or earlier when updated KYC information is received. Any additional or updated customer information obtained under

Rule 9(1C) of the PML Rules or para mentioned below, must be submitted to CKYCR within seven days or as notified by the Central Government, ensuring CKYCR updates the customer's records and electronically informs all relevant companies. Upon notification from CKYCR, Company must retrieve the updated records and align its KYC records accordingly.

For establishing an account-based relationship, updating/periodically updating customer details, or verifying customer identity, Company shall obtain the KYC Identifier from the customer or retrieve it from the CKYCR. Using this KYC Identifier, Company will access the KYC records online and shall not require the customer to submit the same KYC records, information, or additional identification documents, except in specific circumstances. These include cases where the customer's information in CKYCR records has changed, the retrieved KYC records are incomplete or inconsistent with current KYC norms, the validity of the downloaded documents has expired, or Company deems it necessary to verify the identity or address (including current address), perform enhanced due diligence, or build a suitable risk profile of the customer.

7. UPDATION OR PERIODIC UPDATION OF KYC

Davinta shall periodically update Customer's KYC information / documents after the transaction is entered. The periodicity of updating of Customer's KYC data shall be once in 10 years for low risk customers, once in every 8 years for medium risk customers, and once in 2 years for high risk categories *(categorization of risk mentioned in Annexure-3 of this policy)*, subject to following conditions:

a) Individuals:

No change in KYC information: In order to comply with the requirement mentioned above, if there is no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the company, customer's mobile number registered with the company, ATMs, digital channels (such as online banking / internet banking, mobile application of company), letter, etc.

Change in address: In order to comply with the requirement mentioned above, if there is a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the company, customer's mobile number registered with the company, ATMs, digital channels (such as online banking / internet banking, mobile

application of company), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. Further, Davinta can also obtain a copy of OVD or deemed OVD, as defined in Section 3(a)(xiv), or the equivalent e-documents thereof, as defined in Section 3(a)(x), for the purpose of proof of address, declared by the customer at the time of updation/periodic updation.

Aadhaar OTP based e-KYC in non-face to face mode may be used for updation/periodic updation.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals:

i. **No change in KYC information:** In order to comply with the requirement mentioned above, if there is no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of company), letter from an official authorized by the LE in this regard, board resolution, etc.

ii. **Change in KYC information**: In order to comply with the requirement mentioned above, if there is a case of change in KYC information, company shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

c) Additional measures:

i. The KYC documents of the customer to be as per the current CDD standards of the company. Further, in case the validity of the CDD documents available with the company has expired at the time of updation/periodic updation of KYC, company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

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

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation/ periodic updation. Company to promptly update the records as per information / documents obtained from the customers at the time of updation/ periodic updation of KYC and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

d) Update in-case of PML rules

Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at company's end.

8. RISK MANAGEMENT

a. The Company will strictly comply with the laid down policies on Accounting, Lending, Recovery etc., and also the guidelines issued from Registered Office from time to time.
b. The Company shall ensure that its Audit machinery is staffed adequately with individuals who are well versed with applicable policies and procedures.
c. Registered Office will ensure that all the frontline staff members are kept well informed of the KYC norms and procedures for implementation.
d. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
e. The Company applies a Risk-Based Approach (RBA) for mitigating and managing identified risks, whether identified independently or through national risk assessments. In line with this approach, it has established Board-approved policies, controls, and procedures. A Customer Due Diligence (CDD) program is implemented, taking into account the money laundering and terrorism financing risks identified and the scale of our business operations. Additionally, it continuously monitors the effectiveness of these controls and enhances them as necessary. A detailed approached is mentioned as **Annexue-3.**

9. CUSTOMER EDUCATION

Registered Office/ Corporate Office will be providing specific literature/pamphlets to educate the customers on the objectives of KYC norms and procedures seeking their cooperation in getting the information required from them.

10. INTRODUCTION OF NEW TECHNOLOGIES

Registered Office/ Corporate Office will ensure that necessary control mechanism will be built in the Software packages to be implemented to prevent the use of the technology for money laundering purposes.

11. APPOINTMENT OF PRINCIPAL OFFICER

a. Mr. Ashwini Mehra, director of the Company will be Principal Officer of the Company to coordinate the implementation of KYC norms in the Company.
b. The Principal Officer is authorized to fix the accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines, in consultation with the Chief Executive Officer and/ or Head of Finance of the Company.

12. MAINTENANCE OF RECORDS OF TRANSACTIONS

Davinta shall be maintaining proper record of transactions as per requirements of the Prevention of Money Laundering Act, 2002 atleast for a period of 5 years from the period of transaction, including but not limited to :

a. All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
b. All series of cash transactions integrally connected to each other which have been valued below Rupees ten lakhs where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakhs.
c. All transactions involving receipts by non-profit organizations of rupees ten lakhs 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.

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

Davinta is required to maintain the following information in respect of transactions referred above (1) The nature of transactions; (2) The amount of transactions and currency in which they are denominated ;(3)the date on which transaction was conducted; and (4)the parties to the transaction

13. COMBATING FINANCING OF TERRORISM

- Davinta conducts regular Money Laundering (ML) and Terrorist Financing (TF) risk assessments to identify and mitigate risks related to clients, regions, products, and services. These assessments consider sector-specific vulnerabilities shared by regulators and are documented in proportion to the company's scale and complexity. The frequency of these assessments is set by the Board or its delegated committee, with a mandatory review at least annually. The results are reported to the Board and are accessible to relevant authorities and regulatory bodies as required.

- In terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, Davinta shall ensure that it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists as available under the below links:

- The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen-alqaida.html.

- The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

- Davinta shall ensure referring the lists as available in the Schedules to the Prevention and

Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The said lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis" and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Davinta for meticulous compliance.

- Details of accounts resembling any of the individuals/entities in the list shall be reported to FIU-IND by filing the requisite forms on an applicable due dates, apart from advising Ministry of Home Affairs as required under UAPA notification dated February 02, 2021.

- In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of. In term of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005) and amendments thereto. The Reserve Bank of India (RBI) vide its Circular DOR.AML.REC.111/14.01.001/202324 dated April 28, 2023 and subsequent modifications thereof, have prescribed guidelines for freezing/unfreezing of accounts, financial assets, etc., of individuals / entities designated under the list as specified under Section 12A of the WMD Act, 2005.

- In view of the above amendment, the Davinta complies with the below clauses:

  a) Davinta shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

  b) Davinta shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

  c) In case of match in the above cases, Davinta shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer,

where the account / transaction is held and to the RBI. Davinta shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

d) Davinta may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

e) In case there are reasons to believe beyond doubt, that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Davinta shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX or by post, without delay.

f) In case an order to freeze assets under Section 12A is received by the Davinta from the CNO, Davinta shall, without delay, take necessary action to comply with the Order.

g) The process of unfreezing of funds, etc., shall be carried out as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Davinta along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

As mandated, Davinta shall ensure verification w.r.t., the 'UNSCR 1718 Sanctions List Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list by way of additions, deletions or other changes as amended from time to time by the Central Government.

14. REPORTING TO FINANCIAL INTELLEGENCE UNIT– INDIA

The Company will be reporting the information in the proper format, transactions relating to cash and suspicious nature to the Director, Financial Intelligence Unit- India (FIU-IND) at the following address:

Director,

FIU-IND Financial Intelligence Unit – India 6th Floor,
Hotel Samrat,
Chanakyapuri,

New Delhi – 110 021

1. The information in respect of the transactions referred in PML Rules (i.e. clauses mentioned in section 12 above) is to be submitted to the Director every month by the 15TH day of succeeding month.
2. The information to be submitted to the Director promptly, in writing or by E-mail, or by fax, not later than seven working days from the date of occurrence of such transaction and on being satisfied that the transaction is suspicious.

Principal Officer:

The Company has nominated Mr. Joseph Neri to act as Principal Officer who will submit report to FIU-IND for all the information relating to cash and suspicious transactions.

Designated Director:

The Company has nominated Mr. Gopal Chakravarthy, to oversees the operations of the company, as the Designated Director of the Company under the Prevention of Money Laundering Act,2002 and rules framed thereunder.

Further, the Company has communicated the details of the Principal Officer and designated director such as name, designation and address to the office of the Director, FIU-IND.

ANNEXURE 1

CUSTOMER IDENTIFICATION PROCEDURE

FEATURES TO BE VERIFIED AND DOCUMENTS THAT MAY BE OBTAINED FROM CUSTOMERS

Features	Documents
I. Individuals	
Legal name and any other names used	1. Aadhar Card 2. Pan Card 3. Driving License 4. Identity card 5. Letter from a recognized public authority or public servant verifying the identity and residence of the customer 6. Passport
Correct permanent address	1. Telephone Bill(not more than two months old) 2. Account statement 3. Letter from any recognized public authority 4. Electricity Bill(not more than two months old) 5. Ration card 6. Letter from employer 7. Any one document which provides Customer information to the satisfaction of the entity. 8. Aadhar card 9. Property/Municipal Tax receipt (not more than two months old) 10. Piped Gas/Water Bill(not more than

	two months old)
II. Companies	
Name of the Company - Principal place of business - Mailing address of the Company - Telephones/Fax number	1. Certificate of Incorporation and Memorandum and Articles of Association. 2. Resolution of the Board of Directors 3. Power of Attorney granted to its managers, officers or employees to transact the business on its behalf 4. Copy of PAN of the Company 5. telephone bill(not more than two months old) 6. PAN, Aadhar and other documents as may be considered necessary relating to beneficial owner, managers, officers or employees holding an attorney 7. the names of the relevant persons holding senior management position; 8. the registered office and the principal place of its business, if it is different.
III. Partnership Firm	
Legal Name - Address - Name of all partners and their addresses - Telephone numbers of the firm and partners	1. Registration Certificate, if registered. 2. Partnership Deed. 3. PAN of the Partnership Firm.

	4. Documents as specified in Section 16 relating to the beneficial owner, managers, officers, or employees holding an attorney to transact on its behalf, and a telephone bill in the name of the firm and/or partners (not more than two months old). 5. PAN, Aadhaar, and other necessary documents relating to the beneficial owner, managers, officers, or employees holding an attorney. 6. Names of all the partners. 7. Address of the registered office and the principal place of business, if different.

Note:

1- Beneficial Owner means 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 detailed definition has been provided in the RBI's KYC Direction and Rule 9 (3) of the Prevention of Money Laundering Rules 2005.

2- Officially valid document is defined to mean the passport, the driving license, the Permanent Account Number card, the Voter's Identity Card issued by the Election Commission of India, Letter issued by the Unique Identification Authority of India containing details of name, address or any other document as may be required by the Company.

ANNEXURE-2

ENHANCED DUE DILIGENCE (EDD) MEASURES FOR BELOW-MENTIONED CATEGORIES

1. Accounts of Politically Exposed Persons (PEPs)

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.

1.1 Davinta 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.

1.2 Davinta shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a Customer.

1.3 The decision to provide financial services to an account for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis.

1.4 The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

2. Accounts of non-face-to-face customers

2.1 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.

2.2 Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for.

3. Accounts of companies and firms

Davinta need to be vigilant against business entities being used by individuals as a front for maintaining accounts with NBFCs. It may 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.

ANNEXURE-3

RISK-BASED APPROACH FOR COUNTERING AML/TF:

The Board of Directors of Davinta financial services private limited shall ensure that an effective KYC/AML/CFT 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 of staff and other related matters.

In addition, the following also to be ensured for effectively implementing the AML/CFT requirements:

i. Using a risk-based approach to address management and mitigation of various AML/CFT risks.
ii. Allocation of responsibility for effective implementation of policies and procedures.
iii. Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
iv. Concurrent/internal audit/snap audit to verify the compliance with KYC/AML policies and procedures.

During the onboarding of the customer a proper profiling of the customer should be in place to categorise the customer based on the risk categorisation.

The customer profile may contain information relating to 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 will depend on the risk perceived by Davinta. Davinta shall categorise the customers into low, medium and high risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to.

Davinta shall have a Board approved policy for risk categorisation and ensure that the same is meticulously complied with, to effectively help in combating money laundering activities. The nature and extent of due diligence, shall be based on the following principles:

i. Individuals (other than High Net Worth) and entities, whose identity and source of income, nature of business can be easily identified, shall be categorised as low risk.

ii. Customers who are likely to pose a higher than average risk shall be categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, shall be categorised as high risk.

'Customer risk' in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product and channels used by the customer.

For effective implementation of KYC, anti-money laundering (AML) and combating of financing of terrorism (CFT) measures, Risk categorizing a customer as Low Risk, Medium Risk and High Risk. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, end-use monitoring and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.

While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Defining risk categorization:

1) low risk:
    a. Individuals where the end use of the facility can be monitored.
    b. Business units seeking funds for purchase of goods where the funds are not directly remitted to the customer, rather it is transferred against the purchases made to the pre-approved and qualified beneficiary.
    c. Regular sync of data or transactions available or based on the request.
    d. End to end digital journey being deployed for transactions.
    e. Proprietorship firms with no secondary beneficiary (other than business which is run under dubious names).

f. Business and residence of the borrower is located in the same city.
g. Individuals running only one business which is clearly identifiable.

2) Medium risk:
   a. Immediate family member or related party to the beneficiary.
   b. Partnership, private limited, limited or LLP concerns with or without family holding.
   c. Multiple companies reported under single partner/director.
   d. Individuals engaging in cash transactions (primarily repayment) or the payments are being routed from some third party other than the borrower.
   e. Individuals with multiple business interests.
   f. Partners/directors not residing in the same city.
   g. Individuals where the business and residence is located in different city or geography.
   h. Individuals falling under caution profile.

3) High risk:
   a. Politically exposed persons or where immediate family members (including partners/directors) are politically exposed.
   b. Individuals listed in the negative profile of Davinta.
   c. Individuals who are convicted or having criminal record.
   d. Individuals with direct or indirect association with shell companies.
   e. Individuals or firms with dubious records or negative records which can be accessed through any public domain.
   f. Trusts, charitable organisations and societies which receive donations.
   g. 'Firms' with sleeping partners.
   h. Companies/firms/LLP's where directors are non-residents.
   i. Individuals where V-KYC or Digital KYC cannot be completed.
   j. Any other individuals or business where the end-use of the funds cannot be established.

Davinta has adopted combination of manual and automatic classification. Based on the availability of data, Davinta shall finalize parameters which are available in the system and the same shall be reviewed annually. Davinta shall prepare a profile of the customer based on the risk categorisation and the risk perception.

Risk Parameters:

The first step in process of risk categorization is selection of parameters, which would determine customer risk.

IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used, considering the nature of business activity of Davinta the following parameters can be used to determine the profile and risk category of Customers:

A) Some of the indicative parameters being

i. Customer Constitution.

ii. Business Segment.

iii. Country of residence / Nationality: Whether India or any overseas location / Indian or foreign national.

iv. Economic Profile.

v. Account Status:

vi. Account Vintage:

vii. Transaction risk: behaviour of the customer post the customer has been onboarded.

viii. External risk:

ix. Presence of regulatory risk profiles like PEP/defaulter list.

x. Other parameters like transaction with anchor or platform, source of repayment, utilisation of funds, credit rating, concentration, etc.

Note: Davinta can use all of the above or majority of the parameters based on the availability of the date.

B) Apart from profiling the customer, the transaction of the customer with Davinta also poses additional risk factor which should be in line with the nature of business, based on such transactions, the customer can be classified as follows:

Low risk	Medium risk	High risk
Transaction less than Rs 25L in a FY.	Transactions more than 25L and less than 75L in a FY.	Transactions more than 75L in a FY.

C) Risk categorization of customers shall be based on combination of above parameters, i.e., mentioned under A and B. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer.

Note –Review of the risk rating of the customer will be done periodically, minimum once every year.

Roles and responsibilities:

1) Credit and risk head: the role of the credit and risk head will be to ensure overall compliance of the act and rules, review of the parameters from time to time. Training of various stakeholders in the organisation to ensure that AML and CFT risk is clearly understood and becomes a part of risk based approach during evaluation.
2) Operations Head – The role of the operations head will be to ensure that all KYC (V-KYC/Physical KYC/etc.) are as per the set standards of the Davinta and regulator at all operational level, which are issued from time-to-time.
3) Credit department – credit department will review all accounts based on the severity of the accounts and tag them as low, medium and high risk based on the policy guidelines. Periodic review of the appropriate tags will be done. Credit department will also conduct training to the front line teams to ensure that AML CFT policy is understood in letter and spirit.
4) Zonal Managers – The Role of zonal managers is to effectively monitor the KYC / AML / CFT/ CKYC / Re-KYC compliance at operational units, including overseeing and ensuring overall compliance with regulatory guidelines on KYC / AML / CFT / CKYC / Re-KYC in the Zone , abiding by the policy guidelines and govt. rules and regulations , as amended from time to time.

Transaction monitoring:

DFS is into lending business with specific focus on supply chain finance. In this business, the financing of invoices is based on the underlying transaction between two parties under a trade relationship, post analysis of the underlying trade transaction between the parties through GST invoices raised by the party who is the beneficial owner DFS approves for transaction disbursement. Based on the specific request by the borrower and their authorisation the financing of the transactions is done by DFS. Every transaction and repayment by the borrower is monitored to examine the authenticity of the transaction and thereby such transactions are reported internally.

DFS has board approved policy which defines the segments in which the lending activity can be undertaken, such transactions which are in line with the board approved policy is considered and monitored, transactions which are inconsistent with regards to the specified segment or do not fall under normal course of business are flagged and reported to the risk team, risk team carries out due-diligence WRT to nature of such transactions, type of such transactions and frequency of such transactions.

Periodic review is carried out on such transactions which may impact the overall health of the portfolio which is aligned with the risk category of the customers.

DFS is into lending business with specific focus on supply chain finance. DFS has an approved credit policy which defines specific industries and customer segments to which such loans can be sanctioned. Lending activity is undertaken strictly in line with the approved policy parameters. Deviations, if any, are flagged and approved as per policy.

DFS ensures that such financing are also genuine and end-use is monitored by strictly adhering to the following defined process.

1. Verify genuineness of the underlying invoice.
2. Authorisation by the buyer (borrower) of the invoice and availing the loan.
3. Remittance of each loan tranche directly to the seller.
4. Repayment of the loans are enabled digitally.

As part of the risk management process transactions are also monitored and verified as per policy with ledgers of the sellers or their bank statements