

Know Your Customer (KYC) Policy
Autotrak Finance Limited
January 2019

Contents

CHAPTER 1.....	4
PRELIMINARY	4
CHAPTER 2.....	5
OBJECTIVES & SCOPE OF THE POLICY:	5
CHAPTER 3.....	6
DEFINITIONS:	6
Act and Rules	6
Customer:.....	6
Customer Due Diligence	6
Customer identification.....	6
Central KYC Records Registry (CKYCR)	6
FATCA	6
IGA.....	7
KYC Templates	7
Officially Valid Document (OVD).....	7
On-going Due Diligence	7
Person	7
Principal Officer	7
Suspicious Transaction	7
Transaction	8
Periodic Updation	8
Politically Exposed Persons	8
Wire transfer.....	8
CHAPTER 4.....	9
APPLICATION OF THE POLICY:.....	9
I. Customer Acceptance Policy ("CAP").....	10
II. Customer Identification Procedure.....	12
1. Identification.....	12
2. Verification.....	12
i. Verification through documents:.....	12
ii. Additional verification procedures:	13
3. Resolution of Discrepancies	13
III. Transaction Monitoring and Reporting of Suspicious Transaction.....	14
IV. RISK MANAGEMENT	15
V. TRAINING PROGRAMME:.....	16



VI. RECORD KEEPING:.....	17
VII. APPOINTMENT OF PRINCIPAL OFFICER:	18
VIII. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA:	19
CHAPTER 5.....	20
Periodic Updating of KYC based on Risk Categorisation	20
ANNEXURE I	21
CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)	21
1. Accounts of Politically Exposed Persons (PEPs) resident outside India:	21
2. Trust/Nominee or Fiduciary Accounts:	21
3. Accounts of companies and firms:	21
ANNEXURE II	22
Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers	22
1. Documents for proof of identity and address required for Individuals	22
2. Documents for proof of identity and address required for Proprietorship Concerns	22
3. Documents for Identification and verification of Companies	23
4. Documents for Identification and verification of Partnership firms	23
5. Documents for Identification and verification of Trusts and Foundations	23



CHAPTER 1**PRELIMINARY**

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all Non-Banking Financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies as these being used as the International Benchmark for framing the stated policies, by the regulatory authorities.. In view of the same, Autotrak Finance Limited ("AFL" or "Company") has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures are formulated in line with the prescribed RBI guidelines and duly approved by its Loan & Risk Committee ("Committee").



CHAPTER 2**OBJECTIVES & SCOPE OF THE POLICY:**

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. Thus, the KYC policy has been framed by the Company for the following purposes:

1. To prevent criminal elements from using Company for money laundering activities;
2. To enable Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
4. To comply with applicable laws and regulatory guidelines;



CHAPTER 3**DEFINITIONS:****Act and Rules**

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

Customer:

For the purpose of Company's KYC policy a 'Customer' means a Person as defined under Know Your Customer Guidelines issued by RBI (and any amendment from time to time by RBI) which are at present as under:-

- a) A person or entity that maintains an account and/or has a business relationship with the Company;
- b) A Person who has a Registered Account with Company and has a financial transaction or activity with the Company;
- c) A Person on whose behalf the Registered Account is maintained (i.e. the beneficial owner);
- d) Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law;
- e) Any other Person connected with a financial transaction which can pose significant reputation or other risks to Company, say a wire transfer or issue of high value demand draft as a single transaction.

Customer Due Diligence

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner.

Customer identification

"Customer identification" means undertaking the process of CDD.

Central KYC Records Registry (CKYCR)

Central KYC Records Registry means an entity defined under Rule 2(1)(aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

FATCA

FATCA means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.



IGA

IGA” means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

KYC Templates

“KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

Officially Valid Document (OVD)

Officially Valid Document (OVD) means the passport, the driving licence, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, Aadhar Card and Permanent Account Number (PAN) card.

Explanation 1.-For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

On-going Due Diligence

“On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.

Person

Person shall have the meaning as defined under KYC policy of RBI (and any amendment from time to time by RBI) which at present is as follows:

‘Person’ shall include:

- a) an Individual;
- b) a Hindu Undivided Family;
- c) a Company;
- d) a Firm;
- e) an association of persons or a body of individuals, whether incorporated or not;
- f) every artificial juridical person, not falling within any one of the above person (i to v); any agency, office or branch owned or controlled by any one of the above persons (i to vi).

Principal Officer

Principal Officer means an officer nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

Suspicious Transaction

Suspicious transaction means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith,:

- a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to not have economic rationale or bona-fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

Transaction

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

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

Periodic Updation

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

Politically Exposed Persons

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

Wire transfer

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



CHAPTER 4
APPLICATION OF THE POLICY:

To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. This KYC Policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time. This Policy includes nine (9) key elements:

- i. Customer Acceptance Policy (CAP)
- ii. Customer Identification Procedures (CIP)
- iii. Monitoring of Transactions
- iv. Risk Management
- v. Training Programme
- vi. Internal Control Systems
- vii. Record Keeping
- viii. Appointment of Principal Officer
- ix. Reporting to FIU – India.



I. Customer Acceptance Policy ("CAP"):

1. The Company's CAP lays down the criteria for acceptance of Customers. The guidelines in respect of Customer relationship in the Company broadly includes the following:
 - a) No account is to be opened in anonymous or fictitious/benami name(s)/entity (ies);
 - b) Customer must be a major (i.e. 18 years or above) and must not be incapacitated for entering into a contract as per Indian Contract Act
 - c) Customer must be Indian National.
 - d) Name of the customer should not appear in the list of banned entities as circulated by United Nation Security Council Regulations (UNSCR).
 - e) In case of customers being PEP or becoming PEP subsequently, it is necessary to take approval of senior management without harassment to customer.
 - f) Company will accept Customers only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before opening a new account are to be ensured so 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;
 - g) Company will Classify Customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of Customers. Also, a profile of each Customer will be prepared based on risk categorization. Customer requiring very high level of monitoring, e.g. Politically Exposed Persons as explained in Annexure I may, if considered necessary, be kept in the High Risk Category.
 - h) Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA) and RBI/ Company's guidelines/instructions.
 - i) Company will not open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed, as per the risk categorization, due to non-cooperation of the Customer or non-reliability of the data/information furnished to Company. Suitable built – in safeguards shall be provided to avoid any harassment to Customers.
2. The Company shall prepare a profile for each new Customer during the credit appraisal based on risk categorization as mentioned in this Policy. The nature and extent of due diligence will depend on the risk perceived by Company. At the time of credit appraisal of the Customer the details are recorded along with his profile based on the documents provided by the Customer and verified by Company either by itself or through third party sources. The documents collected will be as per the product norms as may be in practice. However, while preparing Customer profile, the Company shall seek only such information from the Customer which is relevant to the risk category and is not intrusive. Any other information from the Customer should be sought separately with his/her consent and after opening the Registered Account. The Customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes.



3. As per KYC policy, for acceptance and identification, Company's Customers shall be categorized based on perceived risk broadly into three categories – A, B & C. Category "A" includes High Risk Customers, Category "B" contain Medium Risk Customers while Category "C" Customers include Low Risk Customers. None of the Customers will be exempted from Company's KYC procedure, irrespective of the status and relationship with Company or its Promoters.

4. Customer Categorisation

Based on the customer assessment process the customers will be divided into 3 categories based on the perceived risk with customer segment as below:

- i. High Risk – These are the customers classified by the company from time to time with respect of money laundering and collection related challenges i.e. funding to Politically Exposed Persons.
- ii. Medium Risk - These are the customers classified by the company from time to time with respect of risk related to collection i.e. Bar Owners, Collection Agent and Negative Profile Customers.
- iii. Low Risk – Normal customers of the company buying assets genuinely for own consumption/sale of assets or commercial/agriculture hiring.



II. Customer Identification Procedure

1. Identification

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

Each business process shall implement procedures to obtain from each customer, prior to transacting, the following information as may be relevant, to that business:

- a) Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;
- b) For individuals - age / date of birth; For a person other than individual (such as corporation, partnership or trust) - date of incorporation; date of partnership deed
- c) Address including the documentary proof thereof;
 - i. For an individual, a residential or business street address;
 - ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;
- d) Mobile Number/Telephone Number of Customer

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as **Annexure - II** to this policy. These are appropriately covered in the credit policies of the respective businesses and communicated to the credit approving authorities.

2. Verification

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

i. *Verification through documents:*

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in **Annexure - II** to this policy. These are appropriately covered in the credit policies of the respective businesses.



The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as **Annexure – II** to this policy. These should be appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

ii. *Additional verification procedures:*

If applicable, the company will include additional verification procedures to address situations where:

- a) Expired documents issued by Government of India i.e. Driving Licence, Passport or any other documents carrying the photograph of applicant.
- b) The business process associate is not familiar with the documents presented;
- c) Where the business process is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and If the business process cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

3. Resolution of Discrepancies

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.



III. Transaction Monitoring and Reporting of Suspicious Transaction

As a general rule, Company will strive to cap cash remittance by customers to the limit of Rs. 2 lakhs and to advise its customers to use acceptable cashless modes of payment (wire transfer, demand draft, banker's cheque, credit card) to settle their over dues. Acceptance of cash remittance above the limit of Rs. 2 lakhs is subject to written approval of senior management.

Besides, the business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs. 10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.



IV. RISK MANAGEMENT

The Management of the Company under the supervision of the Board of Directors and the Loan and Risk Committee shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures as applicable to Company are implemented effectively. The Company shall 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.



V. TRAINING PROGRAMME:

Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/ staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC Policies and implement them consistently.



VI. RECORD KEEPING:

1. Maintenance of records of transactions: The Company shall maintain proper record of the transactions as required under Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:
 - a) All cash transactions of the value of more than Rupees Ten Lakhs (Rs. 10, 00, 000/-) or its equivalent in foreign currency, though by policy the Company neither accept cash deposits nor in foreign currency.
 - b) All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month.
 - 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; any such transactions.
 - e) All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA.
2. Records to contain the specified information

The Records referred to above in Rule 3 of PML Rules to contain the following information:

- a) the nature of the transactions;
 - b) the amount of the transaction and the currency in which it was denominated;
 - c) the date on which the transaction was conducted;
 - d) the parties to the transaction.
3. Maintenance and preservation of records Section 12 of PML Act requires the Company to maintain records as under:
 - a) records of all transactions referred to in clause (a) of sub-section (1) of Section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of Ten (10) years from the date of transactions between the customers and Company.
 - b) records of the identity of all Customers of Company are required to be maintained for a period of Ten (10) years from the date of cessation of transactions between the Customers and Company .
 - c) Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.



VII. APPOINTMENT OF PRINCIPAL OFFICER:

Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT.



VIII. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA:

The PO shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director, Financial Intelligence Unit India,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi 110021



CHAPTER 5

Periodic Updating of KYC based on Risk Categorisation

Periodic updating shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers



ANNEXURE I
CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

1. 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. Branch/office 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. Branch/office 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 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. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

2. Trust/Nominee or Fiduciary Accounts:

Branch/offices shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the Persons on whose behalf they are reacting, as also obtain details of the nature of the trust or other arrangements in place. The Company 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, branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the Customer Identification Procedures.

3. Accounts of companies and firms:

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with NBFCs. Branch/ office 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 e.g. in the case of a public company it shall not be necessary to identify all the shareholders.



ANNEXURE II

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers**1. Documents for proof of identity and address required for Individuals**

Any one document from the Officially Valid Document (OVD) is only allowed. They are:

- i. Passport
- ii. Driving License
- iii. Permanent Account Number (PAN) card
- iv. Voter's identity card issued by Election commission of India
- v. Job card issued by NREGA duly signed by an officer of the State Government
- vi. Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number

It is implied that proof of address also follows from the above documents only.

A customer shall not be required to furnish separate proof of current address, if it is different from the address recorded in the OVD following documents can be provided by the customer toward address proof:

- i. Utility Bill- Electric/landline phone bill/ Gas Bill of current address (not more than 2 months old).
- ii. Leave and License Agreement/Rent Agreement.
- iii. Property Tax Receipts
- iv. Insurance Payment Receipts
- v. Gas Cylinder delivery Challan

In such cases, a declaration from the customer in application form to be taken indicating the address to which all correspondence will be made.

2. Documents for proof of identity and address required for Proprietorship Concerns

In case of accounts of proprietorship concerns, it has been decided to lay down criteria for the customer identification procedure for account opening by proprietary concerns. Accordingly, apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, COMPANY should call for and verify the following documents before opening of accounts in the name of a proprietary 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 GST / Professional Tax authorities.
- ii. 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.



- iii. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

3. Documents for Identification and verification of Companies

- a) Certificate of incorporation;
- b) Memorandum and Articles of Association;
- c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
- d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

4. Documents for Identification and verification of Partnership firms

- a) Registration certificate;
- b) Partnership deed; and
- c) An officially valid document in respect of the person holding an attorney to transact on its behalf.

5. Documents for Identification and verification of Trusts and Foundations

- a) Registration certificate;
- b) Trust deed; and
- c) An officially valid document in respect of the person holding an attorney to transact on its behalf.

In view of the change in the definition of Officially Valid Documents, henceforth, only the documents mentioned above would be accepted for opening accounts of individuals. Company would not have the discretion to accept any other document for this purpose.

Note:

All the customers namely applicant, co applicants and guarantor shall have valid ID and address proof as prescribed above.

