HITACHI
Inspire the Next

KYC AML Policy

Date	Version	Description	Approved By
28/10/2021	1.0	Original Document	Board of Directors
20/02/2023	1.1	Document Review	Managing Director
15/01/2024	1.2	Document Review	Managing Director

Table of Contents

Abbreviations

Abbreviation	Description
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CCR	Counterfeit Currency Reporting
CTR	Cash Transaction Report
CFT	Combating the Financing of Terrorism
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Action Task Force
FCC	Financial Crime Compliance
FIU	Financial Intelligence Unit
KYC	Know Your Customer
NGO	Non-Governmental Organizations
NSDL	National Securities Depository Limited
ML/TF	Money Laundering/ Terrorist Financing
OFAC	Office of Foreign Assets Control
OVD	Officially Valid Document
PEP	Politically Exposed Person
PMLA	Prevention of Money Laundering Act, 2002
SDD	Simplified Due Diligence
STDD	Standard Due Diligence
RBI	Reserve Bank of India
RFI	Request for Information
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
UBO	Ultimate Beneficial Owner
UN	United Nations

HITACHI
Inspire the Next

1. Introduction

As per the guidelines issued in the 'Master Direction - KYC Direction, 2016' by the Reserve Bank of India on Know Your Customer (KYC) norms, Anti-money Laundering (AML) standards and Combating of Financing of Terrorism (CFT), HPY PA (hereinafter referred to as "the Company") shall undertake steps to implement the KYC/AML/CFT principles. The company shall put in place a board approved policy and shall adopt appropriate procedures to know/understand their customers and their financial dealings

The KYC AML policy shall cover the following four key elements for managing risks prudently:

1.1 Identify the customer
1.2 Verify the customer's true identity
1.3 Understand the customer's activities
1.4 Monitor the customer's activities

For the purpose of this KYC AML Policy, "Customer" means an individual or entity who is a national/ international merchant who avails the payment aggregation or other services offered by HPY PA (Hitachi Payment Services Pvt. Ltd. Payment Aggregator)

2. Objectives, Scope and Applicability

The Company aims to establish and lay down the general framework for identification and acceptance of Customers and to act as deterrent against money laundering and terrorism financing and in turn ensure consistency with FCC obligations. The KYC AML policy has been framed by the Company for the following purposes:

i. To determine the true identity and beneficial ownership of accounts, source of funds, the nature of Customer's business, reasonableness of operations in the account in relation to the Customer's business,
ii. To enable the Company to understand the Customers and their financial dealings more distinctly this in turn will enable the Company to manage the risk more carefully.
iii. To prevent all types of criminal elements from dealing with the Company for any money Laundering Activities.
iv. To control, to detect and report all types of suspicious activities in accordance with the rules and regulations.
v. To comply with all laws and guidelines of the Statutes.
vi. To ensure that the concerned employees are trained in KYC/AML/CFT procedures.

This Policy is applicable for all the offices including the branches that may be opened by the Company from time to time and to be read in conjunction with related operational guidelines issued from time to time. The policy also aims to make all employees aware of their responsibilities and the consequences of non-compliance with this policy. The Senior Management of the Company will be responsible to effectively implement the policy.

3. Governance Framework

3.1 Risk Committee

The Management Committee shall supervise the implementation of the KYC AML Policy framework. A review is conducted by the Committee to spot the weaknesses in the Company's KYC AML framework. This will help the Company to evaluate the effectiveness of the policy and procedures and the implemented changes. They shall be responsible for formulating and periodically reviewing the KYC AML Policy in line with the applicable regulatory guidelines.

3.2 Principal Officer

The Company shall appoint a senior officer to be designated as Principal Officer who shall act independently and report to the senior management. Principal Officer shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer shall oversee and ensure compliance with regulatory guidelines on KYC/AML/CFT issued from time to time.

3.3 Designated Director

The Company shall appoint a Designated Director to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. In addition, it is the duty of the Designated Director to observe the procedures and manner of furnishing and reporting information on transactions related to STR/CTR/CCR. The name, designation and address of the Designated Director is to be communicated to the Director, FIU-IND on any new appointment or change.

4. Key Elements of the Policy

The KYC AML Policy has been framed incorporating the following four key elements:

4.1 Customer Acceptance Policy (CAP)
4.2 Risk Management
4.3 Customer Identification Procedures (CIP)
4.4 Monitoring of Transactions

4.1 Customer Acceptance Policy (CAP)

CAP lays down explicit criteria for acceptance of Customers. The guideline in respect of Customer relationship with the Company broadly includes the following:

i. No account based business relationship will be established in anonymous or fictitious/benami name.
ii. Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done before onboarding to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities or any such individual connected with any terrorists or terrorist activities.
iii. The Company will refrain from entering into a business relationship where identity of the account holder cannot be verified and/or documents/information required cannot be obtained as per the risk categorization, due to non- co-operation of the Customer or non-reliability of the data/ information furnished by the Customer to the Company.
iv. All documents and or information that are to be collected in respect of different categories of Customers depending upon the compliances with the Prevention of Money Laundering Act,

2002 (PMLA) , guidelines of Reserve Bank of India and of the internal policies /rules of the Company.

v. Suitable system is put in place to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the sanctions lists/PEP/ Blacklists.

vi. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

vii. Where an equivalent e-document is obtained from the Customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

viii. Mandatory documents/information shall be sought for at the time of onboarding the Customer and during periodic review. Any additional document shall be obtained only with the explicit consent of the Customer.

4.2 Risk Management

The management of the Company under the supervision of the Board of Directors and Risk Committee shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementations. 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 are implemented effectively.

i. The Company's internal audit shall periodically evaluate the level of adherence to the KYC procedures and comment on the lapses observed in this regard. Audit function shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

ii. The Senior Management shall ensure that appropriate procedures are established and effectively implemented and comment on the lapses observed in the procedures. The Senior Management shall also ensure management oversight over systems and controls, segregation of duties and training of staff.

4.3 Customer Identification Procedure (CIP)

The Company shall obtain sufficient information necessary to verify the identity of each new customer. The Company shall undertake identification of its Customers during the following stages:

i. Commencement of an account-based relationship with the Customer.

ii. When there is a doubt about the authenticity or adequacy of the Customer identification data it has obtained.

iii. When the Company has reason to believe that a Customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand

The nature of information /documents required would depend on the type of Customer. For Customers who are natural persons, Company shall obtain sufficient identification data to verify the identity of the Customer, the address/ location. If the Customer is a Legal person or entity the Company shall:

i. Verify the Legal Status of the Person or entity through the documents that relevant and submitted by them.

ii. Verify that any person purporting to act on behalf of the legal person or entity is so authorised and identify and verify the identity of that person.

The Customer identification requirements as mentioned in Appendix I may be relied upon for Customer Identification.

4.4 Transaction Monitoring

Transaction monitoring is an essential element of effective KYC procedures. The Company shall mitigate risks by understanding the normal and reasonable activity of the Customer in order to identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the Customer.

The Operations team shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible legitimate purpose. The Company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. The transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the Company

Such findings shall be reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-IND) under Department of Revenue, Ministry of Finance.

The format for reporting STR is as follows:

i. https://rbidocs.rbi.org.in/rdocs/content/Pdfs/68787.pdf

5. Risk Categorization

When authenticating or verifying a potential Customer, the Company shall prepare a profile for each new Customer based on risk categorization as per the Board approved policy This shall be done to ensure that the Customers are properly risk assessed before being onboarded. Low, Medium or High level of Due Diligence shall be applied for Customers basis such risk profiling. Records of the Due Diligence procedures performed on each Customer or potential Customer, shall be preserved.

Categorization shall be undertaken based on various factors, such as nature of business/industry, Customer type, business location, volume of turnover, social/ financial status, business longevity, credit history, etc. A system of periodic review of risk categorisation of Customers, with such periodicity being at least once in six months, and the need for applying higher level due diligence measures shall be put in place. Customer rating guidelines based on risk framework used at the time of onboarding and as a part of subsequent due diligence is detailed in Appendix II.

6. Ongoing Monitoring

HPY PA's Risk Team shall perform due diligence on all existing customers periodically, depending on risk categorization of such customers. Ongoing monitoring is an essential element of effective KYC procedures. The Company shall also conduct scrutiny of client's transaction and accounts throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Customer. However, the nature of due diligence shall depend upon the risk perceived by the Company

6.1 Re-KYC

As per RBI guidelines on KYC / Re-KYC, periodic update of Customer identification data including photograph after complying with full KYC norms is required to be undertaken. In addition to the KYC carried out at the time of onboarding, Customers may be required to undergo re-KYC and submit the requisite documents. Any changes in Customer details shall be updated through the Re-KYC process.

The Company shall update KYC data 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. This would involve providing identification and address proof.

6.2 Sanctions Screening

HPY PA shall have suitable systems in place to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the sanction lists circulated by RBI. Screening processes act as a safety mechanism to guard against reputation, operational or legal risks and to prevent the company from being used as a channel for money laundering or terrorist financing purposes. Screening of both existing customers and employees shall be performed at regular intervals.

HPY PA shall scan the Merchants against the following lists published by United Nations Security Council:

i. https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
ii. https://www.un.org/securitycouncil/sanctions/1988/materials

7. Termination of Business Relationship

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the Customer, the Company shall reject the business relationship after issuing due notice explaining the reasons for taking such a decision. Such decisions, however, need to be taken after confirmation from the Chairman & Managing Director or key managerial persons.

The Company shall deactivate the code and all obligations due if they have a match against Sanctions/Blacklists, documents provided are forged/manipulated, the Customer is linked to terrorist or criminal activities.

8. Reporting

8.1 Management Reporting

The Principal Officer shall be responsible for submitting reports on adequacy of the KYC AML risk measurement systems, including any findings of internal and external auditors and advisors to the local senior management or the Board at least every six months. These cases will include, but will not be limited to:

8.1.1 All SARs filed, along with Customer and details;
8.1.2 Customer and relationships rejected/terminated on the grounds of ML/TF activities or financial crime suspicion;
8.1.3 Customers with match against Sanctions or other blacklists; and
8.1.4 Customers with outstanding CDD/identification verifications.
8.1.5 Transaction monitoring alerts
8.1.6 Report on special projects related to regulatory compliance (e.g. elimination of backlog or KYC remediation)

8.2 Regulatory Reporting

The Company will report information relating to suspicious transactions in line with the PMLA Rule 3, 2002. The Principal Officer will provide all the necessary help, to the authorities for any further inquiries and clarifications or for any other purpose for which specific requisitions are made.

The Company shall maintain proper record of transactions as mentioned below:

i. All transactions involving receipts by non-profit organizations of rupees Ten Lakhs or its equivalent in foreign currency.
ii. All cross-border wire transfers of the value of more than Five Lakh rupees or its equivalent in foreign currency whether either original or destination of fund is in India.

The Principal Officer shall report such transactions to:
Director, FIU-IND,
Financial Intelligence Unit- India,
6th Floor, Hotel Samrat, Chanakyapuri, New Delhi – 110021.

9. Records Management

In line with Master Direction – KYC Direction, 2016, HPY PA shall take the following steps for maintaining, preserving and reporting of Customer information:

i. Maintain all necessary records of transactions with Customers including the Merchant agreement, Merchant application, documentation, transaction data, etc. for at least five years from the date of transaction.
ii. Preserve the records pertaining to the identification of the Customers and their addresses obtained while onboarding the customer and during the course of business relationship, for a period of five years from the date of cessation of the transactions.
iii. Make available the identification records and transaction data to the competent authorities upon request.
iv. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
    - the nature of the transactions;
    - the amount of the transaction;
    - the date on which the transaction was conducted; and
    - the parties to the transaction.
v. Evolve a system for proper maintenance and preservation of Customer information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

10. Internal Training

The Company on an ongoing basis shall educate the front-line staff, the compliances staff and the new joiners on the elements of AML / KYC through various training programmes and emails. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new Customers. The Company ensures that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. Such trainings shall be given at the time of onboarding of employees and at regular intervals for sustainable awareness.

11. Secrecy Obligations

11.1 The company shall maintain secrecy regarding the customer information.

11.2 Customer information collected shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the explicit permission of the customer.

11.3 While considering the requests for data/information from Government and other agencies, the company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

11.4 The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of bank requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

12. Audit and Policy Review

The Company's Operations team shall evaluate and ensure adherence to the KYC Policies and procedures on a regular basis. Such compliance report will be submitted to the Board for review at regular intervals

The policy is reviewed on an annual basis and updated to incorporate changes as per RBI Guidelines. All updates/changes to the Policy will be communicated to the relevant staff/relevant stakeholders on a periodic basis. All such changes /modifications will be reported to the Board for approval.

Appendix I – Entity Wise Document List

Particulars	Specific Checks
Individual Checks	
PAN Card / Form 60	• PAN Number is validated by third-party vendor • Collected for Ultimate Beneficial Owner (UBO) and/or Authorised Signatory and/or Power of Attorney and/or Authorisation holder
Officially Valid Document (OVD): (Any 1) Passport, driving license, proof of possession of Aadhaar number, the Voter's Identity Card, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register.	• Aadhaar Card is authenticated via Aadhaar XML • Collected for Ultimate Beneficial Owner (UBO) and/or Authorised Signatory and/or Power of Attorney and/or Authorisation holder • Match all details on OVD with that on PAN (e.g.: name, birthdate, image, etc.)
Individual Address proofs (if required): Utility bills, Property/Municipal Tax receipts, Pension orders and Letter of allotment	• Match name and address with PAN and other documents • Match address proof with details provided during sign-up
Proof of address of foreign nationals: Any document issued by the Government departments of foreign jurisdictions and/or letter issued by the Foreign Embassy or Mission in India.	
Cancelled Cheque	• Bank Account details are verified using Penny Drop
Legal Entity Checks	
Company • Certificate of Incorporation • (MoA) and (AoA) • PAN Card • Board Resolution • Ownership Structure and UBO declaration • OVD of Authorised signatory • Cancelled Cheque	• Verify name, CIN/DIN/LLP via MCA Portal • Board Resolution is verified by matching authorised signatory details on AoA, MoA • OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop
Partnership/Limited Liability Partnerships (LLP) • Registration Certificate • PAN	• Registration checks based on available databases • OVD of Authorised signatory is verified as mentioned above

• Partnership Deed/LLP agreement • Power of Attorney • OVD of Authorised signatory • Cancelled Cheque	• PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop

Sole Proprietorship
• PAN and OVD of proprietor
• Any two of the below documents as proof of business
  ○ Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
  ○ Registration Certificate
  ○ Sales and income tax returns.
  ○ 36CST/VAT/ GST certificate (provisional/final).
  ○ Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
  ○ IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
  ○ Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
  ○ Utility bills such as electricity, water, landline telephone bills, etc
• Cancelled Cheque
	• OVD of Authorised signatory is verified as mentioned above
	• PAN Number is validated by third-party vendor
	• Registration checks based on available databases
	• Bank Account details are verified using Penny Drop

Trusts • Registration Certificate • PAN Card • Trust Deed • Power of Attorney • OVD of Authorised signatory • list of beneficiaries, settlors and trustees • Cancelled Cheque	• Registration checks based on available databases • OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Bank Account details are verified using Penny Drop
Unincorporated Association or a body of individuals • PAN Card • Power of Attorney • Resolution of the managing body • OVD • Cancelled Cheque	• OVD of Authorised signatory is verified as mentioned above • PAN Number of the Company is verified as mentioned above • Registration checks based on available databases • Bank Account details are verified using Penny Drop

Hindu Undivided Family (HUF) • PAN Card • Resolution of managing body • Power of Attorney • HUF Deed (if applicable) • Cancelled Cheque	• PAN Number of the Company is verified as mentioned above • Registration checks based on available databases • Bank Account details are verified using Penny Drop

Appendix II – Indicative List for Risk Categorization

Low Risk
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 are: • People belonging to lower economic strata of the society whose accounts show small balances and low turnover • Government departments and Government-owned companies • Statutory bodies & Regulators • Business Longevity is > 5 years • Country of business establishment is a part of the list: *https://www.fatf-gafi.org/countries/#FATF*
Medium Risk
Customers that are likely to pose a higher than average risk may be categorized as medium depending on customer's background, nature and location of activity, country of origin, sources of funds and their client profile etc. Illustrative examples of medium risk category Customers are: • Customers whose place of business has a scope or history of unlawful trading/ business activity • Where the customer profile is uncertain and/or doubtful/dubious • Mixed/Negative Social Media feedback • Country of business establishment is a part of the list: *https://www.fatf-gafi.org/countries*
High Risk
High risk Customers are the ones who are very likely to be involved in money laundering. Additional information shall be collected to provide a deeper understanding of Customer activity and to mitigate associated risks. Illustrative examples of high-risk category Customers are: • Politically Exposed Persons (PEPs) of Indian/Foreign Origin • Non face-to-face Customers • Trust, charities, NGOs and Organization receiving donations • Those with dubious reputation as per public information available • Companies having close family shareholding or beneficial ownership • Firms with 'sleeping partners' • Accounts of bullion dealers and jewellers • Business Longevity is < 1 year • No actual sale and adverse media reports • Nature of business/industry is a part of the Prohibited Business List • Country of business establishment is a part of the list: *http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)*

Appendix III – Prohibited Businesses List

1. Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services
2. Body parts which includes organs or other body parts
3. Child pornography which includes pornographic materials involving minors
4. Drugs and drug paraphernalia which includes hallucinogenic substances, illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms
5. Weapons which includes firearms, ammunition, knives, brass knuckles, gun parts, and other armaments
6. Websites depicting violence and extreme sexual violence
7. Bestiality