KNOW YOUR CUSTOMER, ANTI MONEY LAUNDERING & MERCHANT ON-BOARDING POLICY

INDEX

1. BACKGROUND

The Reserve Bank of India ("**RBI**") on February 25, 2016 issued the Master Direction - KYC Directions 2016 (Ref.: RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16) ("**RBI KYC Directions**"). These RBI KYC Directions provide comprehensive instructions and directives to regulated entities ("**RE**") in India to establish and follow a robust 'know your customer' policy and process.

In order to combat activities like money laundering, terrorist financing and other related threats to the integrity of the financial system, RBI under the RBI KYC Directions has also required RE's to comply with requirements under the Prevention of Money-Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("**PMLA**"). In this regard, RE's are required to ensure compliance with PMLA, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks.

Pursuant to paragraph 6 of the RBI PAPG Guidelines, PA's are also required to comply with the requirements under the RBI KYC Directions & PMLA.

RBI has also issued guidelines RBI/2009-10/231 (DPSS.CO.PD.No.1102 /02.14.08/ 2009-10) - Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries, as amended and restated from time to time. ("**RBI PAPG Guidelines**"). These RBI PAPG Guidelines govern the functioning of various payment intermediaries, such as Payment Aggregators ("**PA**") and Payment Gateways ("**PG**"), which play a crucial role in facilitating electronic payment transactions between customers, merchants, and banks. Vide the aforesaid RBI PAPG Guidelines, PAs have also been directed to have a comprehensive board approved merchant onboarding policy in order to outline the eligibility criteria, documentation requirements, and compliance obligations that intermediaries must fulfill to operate in the payment ecosystem.

This Know Your Customer, Anti Money Laundering & Merchant on-boarding Policy (hereinafter referred to as "**Policy**") outlines is being put into place to cover, *inter alia*, the following:

a) put into place the KYC policy to be followed by HIPL, which will take into consideration all factors related to the merchants proposed to be onboarded, including their activities, their personal information, and any other relevant metrics through the know your customer (KYC) process to confirm the identity of the merchants and conducting due diligence, appropriate to their risk profile;

b) put into place a policy covering requirements under the PMLA; and

c) put into place a merchant onboarding policy, which will:

   (i) set out the standard criteria and procedure for onboarding new Merchants onto the platform of the payment aggregator, Hiveloop Internet Private Limited (hereinafter referred to as "**HIPL/ Platform**"); and

   (ii) establish guidelines for Merchant registration, verification and approval, ensuring that only competent and reliable merchant businesses are accepted on to the Platform.

This Policy shall be read in conjunction with relevant regulations issued by the RBI from time to time and in case of any conflicts, applicable RBI laws shall prevail. This Policy document shall be renewed as and when there is a change in process initiated by HIPL or based on the notifications and mandates released by RBI.

2. OBJECTIVES AND PURPOSE

2.1. The objective of this Policy is to establish for the purposes of the applicable laws specified in the preceding paragraphs, guidelines and rules that govern the relationship between HIPL and entities/ business that avails the services provided by HIPL on its platform, https://pay.udaan.com (hereinafter referred to as "**Merchants**").

2.2. The Policy aims to:

a) establish explicit and robust framework for the acceptance, verification and safe on-boarding of Merchants;

b) establish the identity of merchants through reliable and verified documentation, ensuring the legitimacy of their business or financial transactions;

c) conduct a risk-based approach to evaluate the potential risks associated with each merchant, business relationship, and transaction, categorizing them into low, medium, or high-risk profiles;

d) combat money laundering by reporting cash and suspicious transactions to the Financial Intelligence Unit (FIU)-INDIA, a central national agency headed by the finance minister responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions; and

e) regularly monitor merchant transactions and report suspicious activities to relevant authorities in a timely and accurate manner.

2.3. The Policy aims to ensure compliance with transparent and fair business practices, applicable law, rules and regulations while outlining the due diligence procedures and requirements for assessing the suitability and integrity of merchants involved.

2.4. HIPL currently has only such merchants on-boarded who are the group entities of HIPL. HIPL aims to put in place the categorisation/ processes of categorising of merchants into low, medium and high-risk profiles once HIPL aims to on-board such potential merchants.

3. POLICY OUTLINE

3.1. Specifying the 'Senior Management' for the purpose of Compliances:

The Board has identified Mr. Sumit Gupta, Mr. Mohit Ranjan and Mr. Bharat Chaudhary, directors as the Senior Management executive who will be responsible for ensuring compliance with the Policy and any other applicable guidelines/ directions issued by RBI from time to time.

Any takeover or acquisition of control or change in management of the Company shall be communicated by way of a letter to the Chief General Manager, Department of Payment and Settlement Systems (DPSS), RBI,

Central Office, Mumbai within 15 days with complete details, including 'Declaration and Undertaking' by each of the new directors.

3.2. Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements:

The Senior Management shall carry out regular evaluation of the compliance functions prescribed under this Policy and other applicable laws from time to time. Any non-compliance or deviation is to be reported to the Board or its Committee (as applicable).

3.3. Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures:

The Board or any other committee to whom the power has been delegated by the Board shall carry out concurrent/ internal audit on a quarterly basis, to verify the compliance with this Policy and procedures laid herein and shall submit such quarterly audit notes and compliances to the Board or Committee (as and when applicable).

4. MERCHANT ONBOARDING

HIPL aggregates services by banks, Payment Service Providers (PSPs) and other service providers under one platform for Merchants to disburse or collect payments through UPI, debit cards, credit cards, net banking and NEFT / RTGS, identifying the payers who make direct bank transfers using NEFT/RTGS/IMPS using virtual accounts, reconciling and managing exceptional scenarios such as late payment confirmations, double payments and payment failures (hereinafter referred to as "**Service**"). By engaging HIPL for the Services provided by them and accepting payments through them, Merchants have given HIPL the right to use their personal information for the purposes captured under Clause 2 of this Policy.

A Merchant's onboarding journey with HIPL begins when a user expresses an interest in one or more of the Services and continues beyond account activation for tracking periodic updates and continuous due diligence.

Merchant can express interest in Services by sending an email to merchants@hiveloopinternet.com

Merchants will then need to submit a duly signed Merchant Application Form (MAF) and other supporting documents to the email ID provided above.

Once the merchants have provided their business, contact & bank details through the online signup process, they need to provide KYC documents to complete their registration in accordance with accepted KYC policies. Detailed steps in this regard are specified below.

HIPL reserves all rights to approve or disapprove onboarding and/ or extension of Services to any Merchant at its sole discretion.

4.1. MERCHANT ACCEPTANCE POLICY

In relation to Merchant onboarding/ acceptance, HIPL shall undertaking the following:

a) HIPL shall only onboard companies incorporated in accordance with the Indian Companies;

b) HIPL shall not onboard or deal with Merchant accounts with anonymous or fictitious/benami name;

c) HIPL shall not onboard or deal with such Merchants in relation to whom HIPL is unable to carry out appropriate customer due diligence (CDD) measures as per the RBI KYC Directions, either due to non-cooperation of the Merchant or non-reliability of the documents/information furnished by the Merchant;

d) HIPL shall not undertake any account-based relationship with Merchants or process transactions with them without following the CDD procedure in accordance with Policy and applicable laws;

e) HIPL shall not onboard any merchant conducting or suspected of carrying out any business of the nature specified in Annexure A.

f) HIPL shall explicitly specify the mandatory information to be sought for KYC purpose while opening an account and during the periodic updation of the same;

g) additional information, where such information requirement has not been specified in this Policy, shall be obtained with the explicit consent of the Merchant;

h) if an existing KYC compliant Merchant of HIPL desires to open another account with HIPL, there shall be no need for a fresh CDD exercise;

i) HIPL shall follow CDD procedure for all the joint account holders, while opening a joint account (if any);

j) HIPL shall screen and identify the Merchants through the CDD procedure to ensure that the Merchants proposed to be onboarded does not match with any person or entity, whose name appears in the sanctions lists indicated as under chapter IX of RBI KYC Directions;

k) where Permanent Account Number (PAN) is obtained, HIPL shall verify the same from the verification facility of the issuing authority;

l) where any equivalent e-document is obtained from the Merchant, HIPL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000);

m) where Goods and Services Tax (GST) details are available, the GST number of the Merchant shall be verified by HIPL from the search/verification facility of the issuing authority;

n) HIPL undertakes that this Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged; and

o) where HIPL forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off such suspicious Merchant, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

4.2. MERCHANT RISK CATEGORIZATION AND SCREENING

a) HIPL shall undertake background and antecedent check of the Merchants in accordance with the process set out in Annexure B, which may be modified by HIPL as may be suitable for the context and business and regulatory needs.

b) The Merchant's website shall clearly indicate the terms and conditions of the service and time-line for processing returns and refunds.

c) Each prospective Merchant engaged by HIPL will be bucketed into one of the following three categories as per the assessment and risk perception of HIPL:

- Low Risk
- Medium Risk
- High Risk

d) The risk categorization shall be based on parameters such as Merchant's identity, social/financial status, nature of business activity, and information about their business, location, geographical risk covering Merchants 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. The ability to confirm authenticity and veracity of the documents and confirm identity through online or other services offered by the issuing authorities shall also be factored in at the time of considering the Merchant's identity.

e) The risk categorization principles applied and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the Merchants to avoid tipping off the Merchants.

f) The risk categorization would be reviewed, and enhanced due diligence measures would be applied at the discretion of HIPL in the case of higher risk perception of a Merchant.

g) FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc., may also be used in risk assessment of a Merchant.

h) The high-risk Merchant accounts shall be subjected to more intensified monitoring and shall be reviewed at a higher frequency in every six months by HIPL.

i) HIPL shall obtain periodic security assessment reports either based on the risk assessment (large or small merchants) and / or at the time of renewal of contracts.

4.3. MERCHANT IDENTIFICATION PROCESS THROUGH KYC

For onboarding a Merchant, it is necessary to establish the merchant's identity, address, and existence by verifying documents.. For the purpose of verifying the identity of Merchants, HIPL will ask for KYC documents. The documents that need to be submitted depend on the constitution type of the merchant and documents HIPL will obtain from different types of merchants are enumerated in Annexure C annexed to this policy. HIPL may at any time seek such additional information or documents as it may deem necessary at the time of onboarding a Merchant or at any time during the Merchants association with HIPL. . HIPL may also rely on Merchant due diligence done by a third party in accordance with the RBI KYC Directions, subject to the following conditions:

a) Records or the information of the merchant due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

b) Adequate steps are taken by HIPL to satisfy itself that copies of identification data and other relevant documentation relating to the merchant due diligence requirements shall be made available from the third party upon request without delay.

c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with merchant due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act

d) The third party shall not be based in a country or jurisdiction assessed as high risk.

e) The ultimate responsibility for merchant due diligence and undertaking enhanced due diligence measures, as applicable, will be with HIPL.

4.3.1. PERIODIC UPDATION

HIPL shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk merchants, once in every eight years for medium risk merchants and once in every ten years for low-risk merchants from the date of opening of the account/ last KYC updation.

a) Individual Merchants

(i) For no change in the KYC information, a self-declaration from the Merchant shall be obtained through the Merchant's email-id or mobile number registered with HIPL, ATMs, digital channels, letter, etc.

(ii) For change only in the address details of the Merchant, a self-declaration of the new address shall be obtained through Merchant's email-id or mobile number registered with HIPL, ATMs, digital channels, letter, etc., and the declared address shall be verified through positive confirmation within two months, through address verification letter, contact point verification, deliverables, etc. HIPL may also obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for proof of address declared at the time of periodic updation.

(iii) For Merchants for whom account was opened when they were minor, fresh photographs shall be obtained upon them becoming a major and at that time it shall be ensured that CDD documents are available with HIPL. Wherever required, HIPL may also choose to carry out fresh KYC of such Merchants.

(iv) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. Where the current address differs from the Aadhaar address, declaration of the current address is not required in this scenario. In order to avoid fraud, HIPL shall ensure that the phone number used for Aadhaar authentication matches the one on file.

b) Merchants other than individuals

(i) For no change in the KYC information of Merchants who are Legal Entities (hereinafter referred to as "LE"), a self-declaration shall be obtained through the registered email id,

ATMs, digital channels, letter from an authorized official, board resolution, etc., and HIPL shall ensure that beneficial ownership information available with them is accurate and update the same, if required, to keep it up-to-date.

(ii) For change in KYC information, the Company to undertake the KYC process equivalent to that applicable for Onboarding a new LE Merchant.

c) Additional Measures:

(i) HIPL shall ensure that KYC documents of the Merchant as per the current CDD standards are available, even if there is no change in Merchant information. If the validity of the CDD documents available has expired at the time of periodic updation, the KYC process equivalent to that applicable for Onboarding a new Merchant shall be undertaken.

(ii) Merchant's PAN details, if available with HIPL, are verified from the database of the issuing authority at the time of periodic updation of KYC.

(iii) For carrying out periodic updation, an acknowledgement is shall be provided to the Merchant with the date of receipt of the document(s), including self-declaration. Further, information obtained from the Merchants at such time shall be promptly updated in the records of HIPL and an intimation, with the date of updation is provided to the Merchant.

(iv) HIPL may make periodic updation available at any branch, in terms of this Policy.

(v) Any additional and exceptional measures adopted by HIPL, which otherwise are not mandated such as requirement of obtaining recent graph, physical presence of the merchant, periodic updation only in the branch office where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc.

4.4. SCRUTINY AND ONBOARDING

(i) Post submission of relevant documents, and upon completion of preliminary checks, HIPL will enter into discussions with the prospective merchants for seeking clarifications and reconciling discrepancies in data submitted (if any).

(ii) Thereafter, an in-principal decision to onboard may be communicated to the prospective merchant.

(iii) Pursuant to discussions and successful completion of the review of the prospective merchant and their compliance to the satisfaction of HIPL, the prospective merchant is then required to execute the on boarding / service agreement along with the required KYC documents in accordance with Company's Policy on KYC, AML and CFT Measures, signed as true copy by the authorized signatories.

(iv) Furthermore on-boarding screening of directors, individual promoters, shareholders with more than 25% holding and senior management of the prospective merchant will be carried out as per the company's KYC, AML and CFT Measures policy.

(v) If prospective merchant is a regulated entity registered with any of the regulator viz SEBI, RBI, PFRDA, IRDAI, etc. and local / governmental body, the AML onboarding screening shall not be required.

(vi) On successful completion of verification process & registration of the Merchant, a Secured dashboard shall be provided to the Merchant which can be accessed through the login details sent on the registered email id of the Merchant. The dashboard shall provide different reports related to the transactions carried out at the Merchant level along with the status of the transaction and funds.

4.5. MONITORING OF TRANSACTIONS

HIPL shall on an ongoing basis monitor the merchant already on-boarded by keeping a reasonable watch on their activities, including but not limited to spike in activities, exceeding any threshold prescribed earlier, unusual cross border activities, changes in the website products, frequent updation in merchant profile and adverse media attention.

HIPL shall also undertake due diligence of the Merchants to ensure that their transactions are consistent with their knowledge about the Merchants, Merchants' business and risk profile and the source of funds. Without prejudice to the generality of factors that call for close monitoring, following types of transactions shall necessarily be monitored:

a) large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the Merchant, which have no apparent economic rationale or legitimate purpose;

b) transactions which exceed the thresholds prescribed for specific categories of accounts;

c) high account turnover inconsistent with the size of the balance maintained; and

d) deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

The extent of monitoring shall be aligned with the risk category of the Merchant.

a) High risk accounts are subjected to more intensified monitoring.

b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored. For instance, cases where it is found that a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

HIPL may also consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

If any merchant is found to be availing our services for a business / operation that is categorized as restricted business under any law of India or as per direction of concerned regulator the services rendered to the said merchant will be terminated with the immediate effect.

5. REPORTING & OTHER COMPLIANCES

a) HIPL shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise as per the RBI KYC Directions periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. (hereinafter referred to as "**Risk Assessment**")

(i) This Risk Assessment shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

(ii) HIPL shall properly document the Risk Assessment and ensure that it is proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of HIPL.

(iii) Further, the periodicity of Risk Assessment exercise shall be determined by the Board of HIPL, in alignment with the outcome of the Risk Assessment exercise and shall be reviewed at least annually.

(iv) The outcome of the Risk Assessment exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and shall be made available to competent authorities and self-regulating bodies.

(v) HIPL shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and in this regard. Further, HIPL shall monitor the implementation of the controls and enhance them if necessary.

b) In accordance with the RBI KYC Directions, HIPL shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

c) In accordance with the RBI KYC Directions, HIPL shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do 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).

d) In accordance with the RBI KYC Directions, HIPL shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India.

e) HIPL shall maintain secrecy regarding the Merchant information which arises out of the contractual relationship between HIPL & the onboarded Merchant. Information collected from Merchants for the purpose of opening of account 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 express permission of the Merchant. While considering the requests for data/information from Government and other agencies, HIPL shall

satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions. The exceptions to the said rule shall be as under:

- where disclosure is under compulsion of law;
- where there is a duty to the public to disclose;
- the interest of HIPL requires disclosure; and
- where the disclosure is made with the express or implied consent of the Merchant.

f) In accordance with the RBI KYC Directions and in terms of provision of Rule 9(1A) of the PML Rules, HIPL shall capture Merchant's KYC records and upload onto Central KYC Records Registry (hereinafter referred to as "**CKYCR**") within 10 days of commencement of an account-based relationship with the Merchant. HIPL shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid as per the LE Template released by CERSAI.

g) Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS), HIPL shall submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the scheme prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

h) HIPL shall comply with the below mentioned internal know your employee / staff principles and follow adequate screening mechanism in the personnel recruitment/hiring process.

i) HIPL shall endeavor to ensure that the staff dealing with / being deployed for Know Your Customer (KYC) / Anti Money Laundering (AML) / Countering Financing of Terrorism (CFT) matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally.

j) HIPL shall strive to develop an environment which fosters open communication and high integrity amongst the staff.

k) HIPL shall put in place an on-going employee training program so that the members of staff are adequately trained in KYC/AML/CFT policy where the focus of the training shall be different for frontline staff, compliance staff and staff dealing with new merchants. The front desk staff shall be specially trained to handle issues arising from lack of merchant education.

l) HIPL shall ensure proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues.

5.1 Requirement for Appointment of Designated Director:

a) In terms of Clause 6 of the RBI KYC Directions, HIPL shall appoint a Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and PMLR and shall be nominated by the Board.

b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

c) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

5.2 Requirement for appointment of Principal Officer:

a) In terms of Clause 7 of the RBI KYC Directions, HIPL shall appoint a Principal Officer to ensure compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

c) Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

d) In no case, the Principal Officer shall be nominated as the 'Designated Director.

6. PMLA, 2022 & PMLR, 2005 COMPLIANCES

6.1. VERIFICATION & DUE DILIGENCE

a) HIPL shall verify the identity of its Merchants and the beneficial owners in accordance with section 11A of the Prevention of Money Laundering Act, 2002 (PMLA)

b) HIPL shall practice enhanced due diligence in identification and verification of the Merchants in accordance with section 12AA of PMLA and rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR)

6.2. RECORD MANAGEMENT

The following steps are shall be taken by HIPL for maintenance, preservation and reporting of Merchant account information:

a) maintain all necessary records of transactions between HIPL and the Merchant, both domestic and international, for at least five years from the date of transaction;

b) preserve records pertaining to the identification of Merchants and their addresses while onboarding and during the course of business relationship, for at least five years after the relationship is ended;

c) make the identification records and transaction data available swiftly, to the competent authorities upon request;

d) maintaining proper record of transactions prescribed under Rule 3 of the PML Rules (as mentioned below) so as to permit reconstruction of individual transaction, including:

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

- the parties to the transaction.

e) evolve a system for proper maintenance and preservation of account information so that data can be retrieved whenever requested by the competent authorities; and

f) maintain records of the identity and address of their merchant, and records in respect of transactions referred to in Rule 3 of the PML Rules in hard or soft format.

6.2.1 **Roles and responsibilities**

The collection department shall be responsible for record-keeping and retention of all documents and records of the merchants. The Operations department shall have custody of all original documents collected from the merchant at the time of onboarding. The collection department should have a SPOC identified for the purpose of record tagging and handling and an excel sheet is to be maintained in this regard. The SPOC should maintain a tracker for the movement of all records.

6.2.2 **Record Location:**

The physical documents collected must be stored at Head Offic. The records which are in physical form as well as digital form should also be uploaded to the server apart from keeping a physical copy of the same. The individual SPOC from the department must ensure that records are timely uploaded to the server for safekeeping with the proper naming convention for easy retrieval.

6.2.3 **Storage of records internally**

There will be limited access to the records to certain SPOC's identified from the company or as directed by the respective functional head. The SPOC who is accessing the records for document keeping and retrieval must ensure the following:

a) the document should not be kept with the individual at his workstation once the purpose is over;

b) all documents must be stored in a fully catalogued manner without fail. This will not only help in easy retrieval but will also allow easy handover/ takeover;

c) the individual record keeper for the department shall ensure that the document cabinets should always be locked;

d) the records should never be carried outside the premises without approvals from the department head;

e) in case of electronic records, IT must ensure that all electronic records are access controlled and stored safely; and

f) there should be an identified list of personnel from IT department who are authorized to retrieve and remove electronic media. The off-site storage of business data can be a life-saver during the disaster. The same should be stored and retrieved as per IT security policy laid down in this regard.

6.2.4 **Storage of records with an external agency**

Wherever the storage of records is outsourced to an external agency, the respective functional head shall ensure that the record movement is per the agreement entered into with the external agency. The physical records shall be stored in a systematic manner with respective departments in the order of the starting date to last date of transaction and labeled accordingly to facilitate identification at the time of shifting to storage vendor place or destruction. Department SPOC should maintain the list of all records handed over to the vendor. Audit department should conduct a sample verification during department /internal audits.

6.3. COMPLIANCE AS PER SECTION 12 & 12A of the PMLA, 2002

(1) HIPL shall

a) maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions and the same shall be maintained for a period of five years from the date of transaction between the Merchant and HIPL;

b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed; and

c) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its client and the same shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(2) Every information maintained, furnished or verified by HIPL save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) HIPL shall furnish the Director appointed under PMLA, 2022 such information as may be required by him.

(4) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section shall be kept confidential.

6.4. COMPLIANCE AS PER RULE 3 OF PMLR, 2005

HIPL shall maintain the record of all transactions including, the record of:

a) all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

c) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;

d) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

e) all suspicious transactions whether or not made in cash and by way of-

(i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:

- cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
- travelers cheques, or
- transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
- any other mode in whatsoever name it is referred to;

(ii) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-

- payment orders, or
- cashiers cheques, or
- demand drafts, or
- telegraphic or wire transfers or electronic remittances or transfers, or
- internet transfers, or
- Automated Clearing House remittances, or
- lock box driven transfers or remittances, or
- remittances for credit or loading to electronic cards, or
- any other mode of money transfer by whatsoever name it is called;

(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of:

- subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, interbank participation or any other investments in securities or the like in whatever form and name it is referred to, or
- purchase and negotiation of bills, cheques and other instruments, or
- foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
- letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

(v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

f) all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India; and

g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

7. REVIEW OF THE POLICY

Any amendments/changes in the Policy shall be approved by the Executive Directors of the Company. Material amendments/changes made in deviation from the current policy shall be placed before the Board of Directors of the Company on a periodic basis, at subsequent board meetings.

ANNEXURE A

PROHIBITED BUSINESS CATEGORIES

Enumerated below are the list of restricted businesses which the merchants are prohibited from entering into:**Adult Products**	Adult goods and services which include pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services and massage parlors: Payment of potentially sexual related services.
Copyrights	Copyright unlocking devices which include Mod chips or other devices designed to circumvent copyright protection. Copyrighted media which includes unauthorized copies of books, music, movies, and other licensed or protected materials Copyrighted software which includes unauthorized copies of software, video games and other licensed or protected materials, including OEM or bundled software
Fake Certificate:	Government IDs or documents which include fake IDs, passports, diplomas, and noble titles.
Drugs:	• Drugs and drug paraphernalia which include illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms. • Unlawful Sale of Prescription Drugs: Online sale of prescription drugs to consumers by a pharmacy that is not, either. • certified by VIPPS® (Verified Internet Pharmacy Practice Sites) or • licensed by the board of pharmacy in the state in which it is located. • Drug test circumvention aids which include drug cleansing shakes, urine test additives, and related items • Prescription drugs or herbal drugs or any kind of online pharmacies which include drugs or other products requiring a prescription by a licensed medical practitioner.
Replica Products:	Counterfeit and unauthorized goods, which include replicas or imitations of designer goods; items without a celebrity endorsement that would normally require such an association; fake autographs, counterfeit stamps, and other potentially unauthorized goods.

Gambling:	Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, and related content. Casino Gaming Chips, Off-Track Betting and Wagers at Racetracks.
Sharp objects:	Weapons, which include firearms, ammunition, knives, brass knuckles, gun parts, and other armaments.
Tobacco and Cigarettes:	Tobacco and cigarettes, which include cigarettes, cigars, chewing tobacco, and related products and Unlawful Sale of Tobacco: Online sale of tobacco products by a retailer that is not (1) Certified to pay state taxes, and/or (2) preventing sale of tobacco products to under-age consumers.
Live Plants/ Animals:	• Endangered species which include plants, animals, or other organisms (including product derivatives) in danger of extinction • Live animals or hides/skins/teeth, nails, and other parts etc. of animals.
Currencies:	• Wholesale currency which includes discounted currencies or currency exchanges • Merchant dealing in Crypto Currencies
Human Parts:	• Body parts which include organs or other body parts
Online Trading:	• Securities that include online trading of stocks and bonds etc.
Devices:	• Cable descramblers and black boxes which include devices intended to obtain cable and satellite signals for free. • Pyrotechnic devices and hazardous materials which include fireworks and related goods; toxic, flammable, and radioactive materials and substances. • Traffic devices, which include radar detectors/jammers, license plate covers, traffic signal changers, and related products
Offensive goods:	• Promote intolerance or hatred. o a. Defame or slander any person or groups of people based on race, ethnicity, national origin, religion, sex, or other factors. o b. Encourage or incite violent acts. o c. Promote intolerance or hatred. • Offensive goods, crime which include crime scene photos or items, such as personal belongings, associated with criminals.
Alcohol:	which includes alcohol or alcoholic beverages such as beer, liquor, wine, or champagne.
Child pornography:	which includes pornographic materials involving minors
Hacking and cracking:	Materials which include manuals, how-to guides, information, or equipment enabling illegal access to software, servers, websites, or other protected property.
Illegal goods:	Which include materials, products, or information promoting illegal goods or enabling illegal acts.
Miracle cures:	Which include unsubstantiated cures, remedies or other items marketed as quick health fixes

Medical Marijuana Dispensary:	Seller of marijuana used for medicinal purposes.
Regulated goods:	Which include air bags; batteries containing mercury; Freon or similar substances/refrigerants; chemical/industrial solvents; government uniforms; car titles; license plates; police badges and law enforcement equipment; lock-picking devices; pesticides; postage meters; recalled items; slot machines; surveillance equipment; goods regulated by government or other agency specifications
Multi-level Pyramid Selling:	• Multi-level marketing system which uses one or more of the following practices which may be considered deceptive: o a. Participants pay money for the right to receive compensation for recruiting new participants. o b. A participant is required to buy a specific quantity of products, other than at cost price for the purpose of advertising, before the participant is allowed to join the plan or advance within the plan. o c. Participants are knowingly sold commercially unreasonable quantities of the product or products (this practice is called inventory loading) o d. Participants are not allowed to return products on reasonable commercial terms. o e. Other Payment Service Providers (except to the extent the entity itself sells goods to which it has title): payments services providers (PSP), Other merchant aggregators.
Matrix sites:	Work-from-home/earn online.
Bureau de Change Establishments:	Ability for card members to purchase Foreign Exchange currency.
Cheque Cashing / Guarantee:	Card member (Merchant) can transact cheque for cash using American Express as a check guarantee card.
Condo (Real Estate) Down Payments:	Payments to other debt related real estate products
Debt Collection:	Collection Agencies, Factoring Companies, Liquidators, Bailiffs, Credit Restoration Services and Bankruptcy Lawyers.
Door to Door Sales:	Unsolicited vendors with immediate payment expected.
Investment on futures maturity/value of goods:	Investment made on futures maturity of goods/Services with an intention of gaining return on investment. (E.g. stock market, wine future, horse breeding, or timber investment).
Leasing Merchants:	Payments to other debt related real estate products. Leasing Merchants (US)
Mortgage Payments:	Payments to other debt related real estate products, Mortgage Payments (US).

Political Parties:	Donations
Telecommunications Services:	Including wireless, cable, satellite, wire line, ISP, Calling Cards, Long Distance Phone/Card reader, Airplane Telephones, Cellular Products/Services.
Mobile point of sale:	Electronic point of sale terminal.
Unregulated Charities:	Merchant that does not have a Tax exemption or local council registration number.
Card member Activated Terminals:	Road Tolls, Car Parking Lots and Garages, Petrol Pumps, Cinema Kiosks, Railway Self-Service Ticketing.
Internet Auctions:	Any form of auctioning carried out on the Internet (excluding North America region).
Internet Electronic Delivery:	Merchants (including E-tickets that are redeemable in person) and Internet Electronic Services.
Night Club:	Related (e.g. Night Club Hostess, Night Club Lounges, Disco, or Gentlemen's Club).
Premium Rate Telephone Services:	all 1-900 lines.
Timeshares:	The selling of part ownership of a property for use as a holiday home, whereby a card member can buy the right to use the property for the same fixed period annually.
PC support services:	Providing diagnostic, troubleshooting, maintenance and repair services to a computer or similar device.
Franchisee Services:	A party (franchisee) acquired to allow them to have access to a business's (the franchiser) proprietary knowledge, processes, and trademarks in order to allow the party to sell a product or provide a service under the business's name.
Any product or service:	Which is not in compliance with all applicable laws and regulations whether federal, state, local or international including the laws of India.

The above list is indicative in nature and may include any such business which is prohibited under any law of India or as per direction of concerned regulator or as may be decided by HPL from time to time.

ANNEXURE B

BACKGROUND AND ANTECEDENT CHECKS

(A) AT THE TIME OF ONBOARDING

(i) Check the company name, director names and key personnel name on Internet for :
- negative Media coverage
- Police compliant /Ongoing Criminal proceeding
- Any fraudulent activity

This will be via simple online check

(ii) Credit background check via corporate CIBIL or equivalent bureau

(iii) Confirm whether merchant's website clearly indicate the terms and conditions of the service and timeline for processing returns and refunds

(iv) In case of a Private or public limited company, download the filings from MCA to validate "no default" on MCA and latest accounts have been updated

(v) Check any past instances of Merchant duping customers or selling fake/counterfeit/prohibited products

(vi) Check to ascertain whether the merchant is engaged in any of the prohibited activities enumerated in Annexure A

(B) ON A PERIODIC BASIS

(i) Activities of the nature specified in paragraph 4.5

(ii) regular checks with regulatory databases and risk categorization of our Authorized Signatory and Beneficial Owners

(iii) The periodicity of such checks shall be as may be decided by the Company from time to time.

ANNEXURE C

KYC DOCUMENTATION PROCESS

1.	**CDD for Individual** For undertaking CDD of an individual, following documents shall be obtained: a) Any one of the following: **(aa)** Aadhaar number[1]. If Aadhaar No is obtained, following are the additional compliances: (i) Aadhaar number shall be authenticated using e-KYC authentication facility provided by UIDAI. If the Merchant wants to provide a current address which is different from the address in the Central Identities Data Repository, self-declaration to that effect can be collected. (ii) if an individual wants to receive a benefit or subsidy, but e-KYC authentication cannot be performed due to injury/ illness /infirmity etc., offline / verification by obtaining the certified copy of any other OVD or the equivalent e-document thereof shall be carried out. CDD done in this manner is shall be carried out by an official of the Company and this shall form a part of their concurrent audit. The Company shall also duly record such cases of exception in a centralized exception database. The database shall contain the details of grounds of granting exception, Merchant details, name of the designated official authorizing the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review. **(ab)** proof of possession of Aadhaar number where offline verification can be carried out, provided mandatory offline verification is carried out; **(ac)** proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or equivalent e-document containing details of identity & address. If an equivalent e-document of any OVD is being collected, the Company to verify digital signature per IT Act2 and take a live photo as specified under the RBI KYC Directions. For this, the Company shall carry out verification through digital KYC as specified under RBI KYC Directions;

[1] To be collected if (i) individual wants to receive any subsidy / benefit notified under the Aadhaar Act; or (ii) individual voluntarily submits Aadhaar.

[2] Authentication of electronic records –
(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
Explanation.—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—
(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.
(3) Any person by the use of a public key of the subscriber can verify the electronic record.
(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

	(ad) KYC Identifier with explicit consent of the Merchant to download records from CKYCR. Record in such cases shall be retrieved online from CKYCR. b) the Permanent Account Number ("**PAN**") or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and c) such other documents / equivalent e-documents as may be required by the Company. CDD of an individual can also be carried through V-CIP, and in such cases the process specified in S. No. E below shall be followed.
2.	**CDD for Companies** For Onboarding a company, certified copies of each of the following or the equivalent e-documents shall be obtained: a) certificate of incorporation; b) memorandum and Articles of Association; c) PAN of the company; d) a resolution from the Board of Directors ("**Board**") and power of attorney granted to its managers, officers or employees to transact on its behalf; e) documents, specified in S. No. 1 (under C(I)), relating to Beneficial Owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf; f) the names of the relevant persons holding senior management position; and g) the registered office and the principal place of its business, if it is different.
3.	**CDD for all Entities other than Natural Persons** For Onboarding a legal person who is not a natural person, the Beneficial Owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of PML Rules[3] to verify his/her identity shall be undertaken keeping in view the following:

Secure Digital Signature –
If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—
(a) unique to the subscriber affixing it;
(b) capable of identifying such subscriber;
(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated,
then such digital signature shall be deemed to be a secure digital signature.

[3] The beneficial owner shall be determined as under—

[3] The beneficial owner shall be determined as under—

(a) where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or has ownership of entitlement to more than fifteen per cent. of capital or profits of the partnership or who exercises control through other means.
(b) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s) as given in clause (a) above.

	a) Where the Merchant or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or Beneficial Owner of such entities. b) In situations where it is established that the Merchant is acting as trustee, nominee, or any other intermediary in the event of trust/nominee or fiduciary accounts, appropriate proof of the intermediaries identities and the identities of the people on whose behalf they are operating, as well as information about the specifics of the trust or other arrangements in existence, must be obtained.

Documents collected from Merchants by HIPL in furtherance of the Merchant identification process, are utilised to undertake background checks and to ensure the fact that such Merchants do not have any mala fide intentions to deceive any of the parties involved.

(c) where no natural person is identified under (a) or (b) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
(d) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
(e) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.