ANTI-MONEY LAUNDERING POLICY

This Anti-Money Laundering Policy ("**AML Policy**") is testimony to the Company's commitments against money laundering, financing of terrorism, and related illegal activities. It describes the Company's policies and procedures instituted to ensure that the Services offered by the Company are not being used by the Users to facilitate commission of any criminal offences, including but not limited to those under the Prevention of Money Laundering Act, 2002 and the Unlawful Activities Prevention Act, 1967. Although under the said laws, the Company does not qualify as an entity obligated to follow the procedures prescribed herein, the Company has prepared this AML Policy to ensure the transparency and to ensure the prevention of money laundering and other illegal activities.

The terms "We", "Our", "Company" and "Us" refer to the Company, and the terms "User", "You" and "Your" refer to a User of our Online Platforms.

This AML Policy applies uniformly to any User desirous of availing the Services or otherwise using or benefitting from the use the Online Platforms and may be read as a part of the User Terms and Conditions. It is imperative that you read this AML Policy before using the Online Platforms or submitting any personal information. By using the Online Platforms, you are expressly consenting to be bound by the User Terms and Conditions and consequently this AML Policy.

1. DEFINITIONS

1.1. In this AML Policy:

"Beneficial Owner" means:

(i) In case of companies, the natural person who has ownership of over 25% (twenty five per cent) of the shares, is entitled to over 25% (twenty five percent) of the profits, or has the power, directly or indirectly, to appoint or elect more than half of the board of directors of such company, as the case maybe;

(ii) In case of partnership firms/Limited Liability Partnerships, the natural person who has ownership of over 15% (fifteen per cent) of the capital or is entitled to over 15% (fifteen per cent) of the profits of such firm, as the case maybe;

"Identification Document(s)" refers to:

(i) Permanent Account Number (PAN) card; or Tax Number

(ii) Aadhaar Number; or Social Security Number given by respective government of respective countries.

(iii) Passport, Driving License, Government issued identity cards; or

(iv) such other document as may be notified by the Company from time to time;

"Periodic Updation" refers to undertaking the User's identity verification afresh by following the procedure prescribed under Clause 8.1 (*Customer Verification Procedure)* of this AML Policy, at such intervals as the Company deems fit or as directed by appropriate enforcement authorities.

"Sanction Lists" refer to lists of natural and juridical persons included under any list circulated by the Reserve Bank of India and the United Nations Security Council, including without limitation, the ISIL and Al-Qaida Sanctions List and the 1988 Sanctions List and any other Sanctions List updated/issued by respective countries.

"Suspicious Transactions" refers to the following activities, whether attempted or executed:

(i) Terrorist financing: transactions which to a person acting in good faith appear to be any funds collected to be used, in full or in part, by any terrorist or related organization, or in order to carry out any of the activities relating to terrorism, or terrorist acts;

(ii) Unusually Complex: transactions which to a person acting in good faith appear to have been structured in a manner of unusual or unjustified complexity;

(iii) Malafide Purpose: transactions which to a person acting in good faith appear to have not been transacted for bonafide purpose or have a sound economic rationale.

(iv) Money Laundering: transactions which to a person acting in good faith appear to involve proceeds of any offence listed in the Schedule to the Prevention of Money Laundering Act, 2002.

1.2. The capitalized terms used herein, but not defined, shall have the meaning given to such terms in the Terms (defined below).

2. AML Policy Is Part Of Our Terms

This AML Policy is a part of and incorporated within, and is to be read along with the User Terms and Conditions (the "**Terms**").

3. Policy Changes

The Company may change and update this AML Policy from time to time. Such changes may be made without prior notice, but any changes will only apply to activities and information on a going forward, not retroactive basis. You are encouraged to review this AML Policy whenever you access the Online Platforms.

4. Your Obligations

4.1. You acknowledge that it is your duty to ensure compliance with the terms and conditions described in this AML Policy and accord your consent to not using the Services and the Online Platforms in any manner which results in committing/attempting to commit any criminal offences. You also agree and consent to any changes made to this Privacy Policy in due course and without notice.

4.2. You must ensure that any personal information and/or Identification Documents submitted by you belong to you.

4.3. You must file a fresh proof of address within six months of making any changes to the address mentioned as per the 'proof of address' submitted by you.

4.4. In case you are acting on behalf of a juridical person, you must identify the Beneficial Owner and also assist in verification of the identity of such Beneficial Owner and any individual who purports to act on behalf of such juridical person.

5. **PURPOSE OF THIS POLICY**

In order to mitigate its risks relating to money laundering and other illegal activities, the Company intends to put in place this policy which has the following elements:

(i) Customer Acceptance Terms; and
(ii) Risk Management Procedure; and
(iii) Customer Verification Procedure; and
(iv) Transaction Monitoring Terms

6. **CUSTOMER ACCEPTANCE TERMS**

6.1. The Company may either at the time of opening the User Account, or while undertaking any transactions, or during Periodic Updation, or for any other reason, ensure your compliance with the following:

(i) Require that you undergo a verification process during the activation process of your User Account by submitting your Identification Documents and such other details, as mandated under Clause 8 (*Customer Verification Procedure*) of this AML Policy;
(ii) Require you to furnish such other details as may be deemed necessary by the Company to verify your identity, if the Company has reason to believe that you are a person or entity enlisted in the Sanctions Lists.
(iii) Require you to submit such additional information and/or data as may be directed by a competent enforcement authority.
(iv) Require you to certify that your Linked Bank Account is held only with a scheduled commercial bank compliant with all Know Your Customer (KYC) procedures mandated under the applicable laws.

6.2. The Company may, in its sole discretion, refuse to open any new accounts, terminate existing User Accounts after giving due notice, or refuse to process any transactions on the Online Platforms if it is unable to ensure compliance with any of the aforementioned conditions, either due to non-cooperation by the User or due to the details provided by the User being found enlisted on any Sanctions Lists or unreliable or unverifiable to the Company's satisfaction.

7. **RISK MANAGEMENT PROCEDURE**

The Company may categorize its Users including you into low, medium or high risk categories, after undertaking an appropriate risk assessment of each User based on the following factors (including without limitation):

- Sufficiency and adequacy of identification information submitted under Clause 8 (*Customer Verification Procedure*); or
- Its social and/or financial status; or
- Nature of User's business/vocational activities; or
- Guidance notes circulated by various governmental and inter-governmental organizations.

You acknowledge that in order to maintain the integrity of the Risk Management Procedure, the Company will keep your risk categorization and any data related thereto confidential. You will not be entitled to seek disclosure of your risk categorization. However, the Company may disclose the User's risk categorization data to the competent enforcement authority if it finds that a particular User has executed or is likely to execute any Suspicious Transaction.

8. CUSTOMER VERIFICATION PROCEDURE

8.1. The Company, during activation of User Accounts or while undertaking any transactions or for any other reason, may require for the purposes of verification of any User's identity, following details:

- In case of individuals - one copy of any Identification Document containing their identity and address details; one recent photograph; any other documents pertaining to business/financial status of such individual as may be prescribed by the Company from time to time;
- In case of companies – one copy each of the Certificate of Incorporation; Memorandum and Articles of Association; Board resolution authorizing to transact on the Online Platform; Identification Documents containing identification and address details of the individual authorised to transact along with a copy of such authorization document;
- In case of partnership firm/Limited Liability Partnership – one copy each of the Registration/Incorporation Certificate; partnership deed; Identification Documents containing identification and address details of the individual authorised to transact along with a copy of such authorization document;

Users must ensure that all copies of aforementioned Identification Documents are duly certified.

8.2. For the purposes of verification of any User's identity, the Company may rely on appropriate and licensed third party service providers to authenticate the Identification Documents and other incidental details provided by the User.

8.3. If the Company finds any User information obtained in accordance with the procedure described under this Clause to be inadequate, insufficient, or enlisted on the Sanctions Lists, the Company may in its discretion either refuse or terminate (as the case may be) the registration of such User Account or require verification of such User's Identification Documents again.

9. TRANSACTION MONITORING TERMS

9.1. All transactions executed and/or attempted to be executed on the Online Platforms are regularly monitored by the Company, both manually and through use of software based algorithms, in order to promptly identify and highlight certain kinds of transaction including without limitation, the following kinds of transactions:

- High value transactions of amounts greater than INR 50,000 (Rupees Fifty Thousand); or Equivalent in USD or any digital asset equivalent of the value INR 50,000 (Rupees Fifty Thousand).

- Cross-border transactions of amounts greater than INR 5 Lakhs (Rupees Five Lakhs); or Equivalent in USD or any digital asset equivalent of the value INR 5 Lakhs (Rupees Fifty Lakhs).
- Suspicious Transactions;

9.2. The Company may, from time to time, undertake necessary investigation in order to identify and examine transactions inconsistent with any User's risk profile (determined in accordance with Clause 7 (*Risk Management Procedure*) above), sophistication, and expected usage pattern.

9.3. The extent of monitoring shall depend on various factors including upon each User's risk profile.

9.4. The Company reserves the right to terminate the User Account, restrict and/or prevent access to Online Platforms, or report to the appropriate enforcement authorities the activities of any User in respect of transactions identified under this Clause 9 (*Transaction Monitoring Terms*).

10. MAINTENANCE OF RECORDS

The Company will maintain and preserve the following information and/or data:

- Records of all transactions executed on the Online Platforms, for a period of at least 10 (Ten) years from the date of each transaction.
- Records of all transactions identified under Clause 9 (*Transaction Monitoring Terms*) above for a period of at least 12 (Twelve) years, including but not limited to the information about the nature, value and parties to such transactions, and their date of remittance.
- Identification records of Users (including but not limited to the Identification Documents submitted pursuant to Clause 8 (*Customer Verification Procedure*) above), during the subsistence of and for a period of at least 10 (Ten) years from the date of termination of such User Account.

11. COMPLIANCE, DISCLOSURE, AND NOTICES

11.1. The Company may share, from time to time, information regarding transactions identified under Clause 9 (*Transaction Monitoring Terms*), identification information of such Users, or any other information mandated under the applicable law, with the appropriate enforcement authorities.

11.2. In order to improve the integrity and transparency of transactions on the Online Platforms, you are encouraged to report any information you are privy to or become privy to in the future regarding any Suspicious Transactions or transactions you have find or have reason to believe are dubious in nature, to our Compliance Officers by writing to them at admin@pyrupay.com.

11.3. In order to ensure compliance with this AML Policy and/or the applicable laws, the Company may be required to send you notices from time to time. All such notices will be

sent to such address as provided by you under Clause 8 (*Customer Verification Procedure*) of this AML Policy. Where you are required to share any information according to the procedures contained in this AML Policy, such communication may be made by you electronically by sending an email to admin@pyrupay.com.