WORLDLINE

WORLDLINE EPAYMENTS INDIA PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC)/ ANTI-MONEY LAUNDERING (AML)/ COMBATING FINANCING OF TERRORISM (CFT) POLICY

WORLDLINE EPAYMENTS PRIVATE LIMITED
2nd Floor, Tower-1, Phase-2, Raiaskaran Tech Park, Sakinaka, Andheri East,
Mumbai City,Maharashtra, 400072. (T) +91 22 66528600 | (F) +91 22 6652 8667
CIN NO: U74200MH2005PTC192623 ; GST NO: 27AABCE4591N1Z6
https://in.worldline.com

Version Number	:	1	Classification	:	Internal
Issue Date	:	February 2021	Process Owner	:	ERM / Compliance

Review History

Version	Name of reviewer	Date of review
1	Execom	February 2021
2	Execom	December 2023
3		
4		

Approval History

This document has been approved by the Board of Directors	
1	March 31, 2021
2	April 05,2022
3	December 18th, 2023

Contents

1. Introduction

Worldline ePayments India Private Limited (hereinafter referred to as 'WEPL' or 'WEIPL' or 'the Company') offers a host of payment solutions that includes Payment Aggregator ('PA') services and other ancillary services. During the provision of these payments services, WEIPL may be exposed to various money laundering and terrorist financing risks and so adequate safeguards are required to be maintained to avoid any such situation.

The Reserve Bank of India ('RBI'), through *Guidelines on Regulation of Payment Aggregators and Payment Gateways,* has drafted the guidelines for regulation payment aggregators. These guidelines also stipulate that provision of the *Master Direction - Know Your Customer (KYC) Direction, 2016 (the Directions)* will be applicable for payment aggregators and PAs are mandated to adhere to the anti-money laundering (AML) laws in the country. In the said context, WEIPL has created a KYC/AML/CFT Policy ('the Policy'). Under this Policy, the Company aims to establish a robust KYC/AML/CFT framework that will always be adhered to while dealing with the stakeholders it may engage with.

For this Policy, the key laws and regulations applicable to the Company are:

- Prevention of Money Laundering Act (PMLA), 2002 and its amendments;
- Prevention of Money Laundering (PML) Rules, 2005 and its amendments;
- Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time; and
- Guidelines on Regulation of Payment Aggregators and Payment Gateways.
- Standards for BHARAT BILL issued by NPCI and its amendments.

PAYMENT SYSTEM
The Board of Directors ('Board') has the ultimate responsibility for the adoption and implementation of the KYC/AML/CFT framework.

For the purpose of this KYC AML Policy, "Customer" means an individual or entity who is a merchant / aggregator and who avails payment aggregation or payment gateway services offered by WEIPL

The KYC AML policy shall cover following key elements for prudent risk management:

- Identify the customer
- Verify the customer's true identity
- Understand the customer's activities
- Monitor the customer's activities

2. Objective and Scope

The purpose of this Policy to enable WEIPL to comply with Reserve Bank Of India's Master Direction on KYC, AML and CFT dated 17th October 2023 for Regulated Entities. The policy covers following key elements for prudent risk management of WEIPL merchant portfolio

- Identify the customer
- Verify the customer's true identity
- Understand the customer's activities

- Monitor the customer's activities/transactions
- Detect and report suspicious activities in accordance with the rules and regulations.

WEIPL will endeavour to prevent from being used, intentionally or unintentionally, by criminal persons or entities for money laundering and other unlawful activities. The Policy covers the Company's approach for customer acceptance, customer identification, risk management, transaction monitoring and overall due diligence. This Policy also provides for the various reporting that WEIPL is required to make to the regulatory authorities.

The provisions of this Policy will apply to all employees, end-users, merchants (including Billers)/customers, third party agents/vendors of the Company as involved in the Payments Aggregation Business and also Biller Aggregation Business under BBPS of the Company

The Policy to be read in conjunction with Merchant Onboarding Policy adopted by the Company, Including all applicable Standard Operating Process notes.

3. Definitions

"Acquiring Bank(s)" means designated bank of the Company with whom it holds escrow account for payment settlement.

"Beneficial means

- Where the customer is a **company**, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For this sub-clause

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
2. "Control" will include the right to appoint the majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

- Where the customer is a **partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership.
- Where the customer is an **unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

- Where the customer is a **trust**, the identification of beneficial owner(s) will include identification of the author of the trust, the trustee, the beneficiaries with 10% 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.

“Card Network Operators” will mean Visa/ MasterCard/ Amex Card/ NPCI/ Diners Club.

"Customer Due Diligence” (CDD) means identifying and verifying the Merchants and the beneficial owner of the Merchant (if any)

"Designated Director” means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Independent evaluation of the compliance functions of REs’ policies and procedures, including legal and regulatory requirements and will include the Managing Director or a whole-time Director, duly authorized by the Board of Directors.

“Merchant Platform” means Merchant Website or Mobile Application of the Merchants

“End-Users” means the person who uses Payment Aggregator service provided by the Company on the Merchant Platform.

“KYC documents/information” means documents mentioned in Annexure I, including Proof of Identity, Proof of Address and such other information/ documents obtained by WEIPL for onboarding merchants.

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

"Principal Officer" means an officer at the management level nominated by company, responsible for furnishing information as per rule 8 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005

“Stakeholders” means Acquiring Bank, Customers/End-users, Merchants, Card Network Operators, Third Party Agents/Vendors, etc. that WEIPL may engage for facilitating PA services.

"Suspicious transaction" means a "transaction" including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence in the Schedule to the Prevention of Money-Laundering Act, 2002, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have an economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

4. Key Elements of the Policy

4.1 Customer Acceptance Policy

For facilitating domestic and/or cross border transactions as a Payment Aggregator, WEIPL shall directly onboard merchants based either in India or abroad or may enter into agreement with e-commerce marketplaces or entities providing Payment Aggregator services domestically or abroad. In all cases it shall be the responsibility of WEIPL to undertake Customer Due Diligence of merchants

WEIPL will not engage with Customers/Merchants undertaking illegal, unethical or brand-damaging businesses, or businesses that are deemed to pose an unacceptable risk to the Company. Resultantly, some of the Customers/Merchants are unacceptable to the Company based on the preliminary parameters viz. industry, business model or location, even before commencing the CDD process. WEIPL will not enter into a business relationship with all such customers. The company will adhere to the principles and ensure the following safeguards while accepting customers:

- No merchant will be accepted in an anonymous or fictitious/benami name.
- No merchant will be accepted where the Company is unable to identify and verify the Merchant, either due to their non-cooperation or non-reliability of the documents/information furnished by them.
- No transaction or relationship will be undertaken without customer due diligence procedure.
- The customer will be informed about the mandatory KYC information that will be required and for periodic updates to be carried out by WEIPL
- Identity of a new customer will be checked to ensure that it does not match with any person with a known criminal background. Additionally, it will be ensured that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists as mandated under Master Direction – KYC by the Reserve Bank of India and updated from time to time and/or as is directed by Financial Intelligence Unit (FIU) and other relevant statutory authorities in India in accordance with the PMLA, 2002 as updated from time to time.

Additionally, the Company will ensure that it does not enter into a business relationship with Customers/Merchants that can be considered to perform unethical activities, whose business practices indicate integrity issues or could be associated with the following activities:

- terrorism or terrorist financing or organized crime
- illicit activities including but not limited to
  - trafficking in narcotics and drug paraphernalia
  - trafficking in weapons (except non-firearms in a peaceful use), goods and merchandise (including anti-personnel mines and/or sub-munitions)
  - use in animals of hormonal substances or trade-in such substances
  - animal wildlife trafficking, trafficking in human beings, human organs, tissues and other human body parts
  - piracy (music, video streaming)
  - being involved in illegal or forced labour
- child pornography, bestiality, rape
- exploitation of prostitution
- fraud detrimental to the financial interests of India
- fiscal fraud, whether organized or not
- embezzlement by public officials and corruption

- environmental crime
- counterfeiting currency or banknotes
- counterfeiting products and infringement of intellectual property rights
- provision of investment, foreign exchange or fund transfer services without authorization
- fraud, breach of trust, abuse of corporate assets, hostage-taking, theft or extortion
- deceptive or false advertising

For merchants engaged in cross border transactions, it shall be ensured that they do not facilitate payment transactions for import of any restricted / prohibited goods and services (not permissible under prevailing Foreign Trade Policy)

4.2 Client identification procedure

Customer Identification Procedure is the process of conducting identification and verification of the customers and the beneficial owners (if any) based on information and documents as appended in the Annexure I to this Policy. The Company will carry out the identification process under the following circumstances:

- At the time of initiation of the relationship with the customer
- When there is uncertainty around the authenticity of the data that has been obtained from the customer
- Where there is suspicion about money laundering or terrorist financing-related activities for an existing customer

4.2.1 Sanctions Screening:

- WEIPL will ensure suitable mechanism and 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 as indicated under the Master Directions on KYC by RBI and/or as is directed by Financial Intelligence Unit (FIU) and other relevant statutory authorities in India in accordance with the PMLA, 2002 as updated from time to time. Screening processes act as mitigant to prevent the company from being used as a channel for money laundering or terrorist financing purposes.

- In addition to screening with sanctions list as mandate by national regulatory and statutory authorities, WEIPL shall also screen its customers with additional specific international lists in alignment with Group Sanctions policy. Risk assessment shall be conducted for customers who are included in the International lists but not in any of the sanction lists mandated by national regulatory and statutory authorities. Response and actioning shall be based on this risk assessment for such cases.

4.3 Customer Due Diligence

While undertaking customer identification, the Company will ensure that decision-making functions of determining compliance with KYC norms will not be outsourced. WEIPL will apply customer due diligence measures to all customers based on the materiality and risk and conduct due diligence on relationships at applicable period.

4.3.1 Following key checks are undertaken as a part of customer due diligence:

- Screening customer details against the UNSCR and applicable Sanctions list in accordance to 4.2.1 of this policy
- Check to determine Acceptance of PEP customers will be approved by Designated Director.
- Check to determine the Ultimate Beneficial Owner (UBO)
- Check against negative lists internally maintained by WEIPL
- Verification of OVDs as specified in the RBI MD-KYC, 2016 as updated from time to time

4.3.2 Identification of Beneficial Owner (BO)

Beneficial Owner as has been defined under clause 2 of Definitions of the Policy. For onboarding of a Legal Person who is not a natural person, the beneficial owner(s) will be identified and all reasonable steps to verify their identity is undertaken.

Format for Beneficial Ownership Declaration is appended in Annexure III

4.3.3 Standard Due Diligence

Simplified due diligence may be applied when the customer is low risk and falls within one of the following categories/ business models:

- Bank-led While label deals
- Government Merchants
- Strategic Alliance Partner (Only Education and Government institutes)

Detailed KYC checklist for the same is mentioned in Annexure III.

4.3.4 On-going Due Diligence

WEIPL will undertake on-going due diligence of customers to ensure that their transactions are consistent with its knowledge about the end-users, merchants' business and risk profile, etc.

- Review and risk assessment of all the Merchants will be conducted every month i.e. Mass Merchant Assessment (MMA) and appropriate due diligence will be implemented accordingly for change in risk categorization from low to medium or high-risk customers.
- A comprehensive review, analysis and risk assessment of top Merchants will be conducted every year and appropriate due diligence will be implemented accordingly for change in risk categorization from low to medium or high-risk customers.

4.3.5 Periodic Updation

Periodic updation of all KYC documents/information of the customers will be carried out at least once every two years for high-risk customers, once every eight years for medium risk customers and once in every ten years for low-risk customers.

4.3.6 Enhanced Due Diligence

Where there is a higher risk of money laundering and terrorist financing, WEIPL will conduct enhanced due diligence. In particular, the Company will increase the degree and nature of monitoring of Merchants, to determine whether activities/

transactions performed by them are unusual or suspicious. Examples of enhanced CDD measures that could be applied to high-risk customer relationships include:

- Obtaining additional information on the customer (for example business details, the volume of assets, information available through public databases, internet etc.)
- Obtaining information on the reason behind suspicious transactions
- Conducting enhanced monitoring of the Merchant by increasing the monitoring on value and volume of the transactions and selecting patterns that need further examination

4.3.7 Engaging with Politically Exposed Persons (PEPs)

While onboarding a PEP as an authorised signatory or UBO the following additional steps will be taken by the Company:

- Identification of the location of the PEP: located in a high-risk country i.e. the Country Risk List or in a country with high levels of corruption
- Obtain any other information concerning the PEP using independent public sources
- Obtain approval from either the Director Risk, if he/she is not available the VP Risk and Compliance, and if he/she is not available one of the Statutory Directors or Designated Director.
- Designated director's approval will be sought for onboarding a PEP and for continuing the business relationship with a PEP and also in the event when an existing customer subsequently becomes a PEP

The level of risk of the PEP must be determined and adequate monitoring is required depending on the risk level of the PEP. The process in the above para (4.3.6) will also be applicable, where a PEP is a beneficial owner.

4.3.8. Due diligence with respect to Cross border transactions:

- In addition to KYC checks and due diligence on the merchant on specific transactions regarding imports of goods and services, WEIPL will ensure due diligence of the buyer above specific thresholds as required by regulatory guidelines updated from time to time

4.4 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.

WEIPL will undertake risk profiling of the customers based on the information/documents collected to enable appropriate assessment of risk and risk categorisation of the customers. The Company will adopt a risk-based classification criterion that categorises customers on factors such as their customer's business, social/financial status, nature of the activity, and information about their business / geographical location etc. Basis stated indicative criteria, the Company will categorise customers into High, Medium and Low risk The risk assessment carried out will consider all the relevant risk factors before

determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment will be documented with periodic updation and will be made available to competent and regulatory authorities , as and when required.

In addition to the standard documentation, additional documents/information may be required by the Company as per the risk categorisation and the risk profile of the Merchant. The Company will also determine the type of due diligence and necessary additional documents/information which will be obtained to conduct a proper risk assessment. List of such additional documents/information is mentioned in Annexure-II.

Based on the risk categorisation, enhanced due diligence will be applied when there are reasons to believe that a higher risk of money laundering and/or terrorist financing exists. The following businesses require enhanced due diligence:

- Merchants with reasons to believe to be involved with money laundering and or terrorism financing (see Annexure IV for a list of red flags/key risk indicators)
- Complex ownership structures, when ownership is held through high-risk countries or tax/secrecy havens
- Charities involving political/religious causes or high-risk countries
- Financial Services, FX brokers/dealers
- Merchants with PEPs located in high-risk countries

“High-Risk” business models need careful evaluation due to the risky nature of the business, which could cause WEIPL financial losses or compliance issues. Following is the list of business models which will be carefully evaluated before WEIPL accepts them as the merchants:

- Multi-Level Marketing schemes or Pyramid / Matrix sites or websites Merchant Platform using a matrix scheme approach.
- Prescription drugs or herbal drugs or any kind of online pharmacies which includes drugs or other products requiring a prescription by a recognized and licensed medical practitioner in India or anywhere else. Gaming which includes, memberships/ enrolment in online gaming sites, rummy, fantasy gaming etc., and related content (Game of skill).
- FOREX – buying, selling and trading.
- Job services.
- Air guns.
- Perishable goods.
- Matrimony services (Not dating).
- Real estate buying/selling/other services.
- Crowdfunding.
- Website hosting.

WEIPL shall also risks arising from Money Laundering and Terrorist Financing

4.5 Ongoing Transaction Monitoring

Monitoring is performed to ascertain that the transactions being conducted are consistent with the Company’s knowledge of the Customer. Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of Merchants Platform & Transactions is

also influenced by merchant risk category, which in turn depends on various parameters such as Merchant Business category, Vintage, Transaction Volumes & Value undertaken by the merchant, chargebacks received etc.

Transaction monitoring is performed for all eligible merchant (eligible merchants are those where WEIPL underwrites credit risk. Merchants wherein WEIPL does not underwrite credit risk are monitored by respective acquiring entities/merchants).

For BBPOU, as a Biller Operating Unit, WEIPL are a recipient of bill fetch and payment request (post successful payment) through NPCI. All the payments are getting processed at Agent/COU end. Hence, transaction monitoring as a scope of activity is not considered for BBPS transactions at WEIPL.

4.6 Key Appointments

The PMLA and PML Rules require the regulated entities to appoint two key personnel to ensure overall compliance with the obligations as specified under the law. The Company will make the following key appointments:

- Designated Director
  WEIPL will nominate a person as the Designated Director to ensure overall compliance with the obligations under the PMLA and PML Rules. The Designated Director will be nominated by the Board of Directors and will perform various functions as required under this Policy and by the relevant authorities.
- Principal Officer
  WEIPL will also appoint a Principal Officer, other than the person appointed as Designated Director, who will be a senior management official. Principal Officer is responsible for ensuring implementation of the provisions of this Policy, making various reporting to FIU-IND and liaising with various regulators.

4.7 Regulatory Reporting

As per the requirement of PMLA and Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules), the following information will be furnished to Financial Intelligence Unit-India (FIU-IND):

Report	Relevant transactions	Due Date
Suspicious Transaction Reports (STR)	• All suspicious transactions identified post transaction screening mechanism and investigated and confirmed for reporting to the FIU-IND by the Principal Officer.	Not later than seven working days from the date of confirmation of suspicion

WEIPL has implemented internal systems and designated internal team of experts who monitor and analyse all the merchant transactions, to notice and observe any unusual transactions patterns for detecting suspicious transactions and furnishing information about such transactions as specified by FIU-IND and RBI. The Principal Officer will furnish

the applicable report mentioned above based on the information available with the Company and retain a copy of such information for an official record.

It is the responsibility of WEIPL and its Designated Director to follow the manner and procedure of furnishing information as specified by FIU-IND/RBI. While undertaking transaction monitoring, the Company will also ensure that Suspicious Transaction Report (STR) reporting is performed in FIU-IND portal FinGate 2.0 within seven days of confirmation of suspicion and . WEIPL will ensure that there is no tipping off to /intimating the Merchants at any level.

4.8 Record Retention

For the purpose of maintenance, preservation and reporting of Merchant KYC documents/information, WEIPL will undertake the following activities:

- Maintain all necessary records of transactions between WEIPL and Merchant, Merchant and their end-users for at least five years from the date of transaction. Necessary information in respect of transactions to permit reconstruction of an individual transaction will also include the following -
  - the nature of the transaction;
  - 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.
- Preserve the records pertaining to the identification of the Merchants obtained while onboarding and during the course of the business relationship, for at least five years after the business relationship is ended;
- Provide the identification records and transaction data to the relevant authorities upon request;
- Evolve a system for proper maintenance and preservation of KYC documents/ information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the relevant authorities; and

5. Other Areas

5.1 Employees' hiring and training

WEIPL will implement an adequate screening mechanism for its employee recruitment/hiring process.

An on-going mandatory employee training programe will be conducted for employees on KYC/AML compliance. The focus of the training will be customised for frontline staff (Sales & Marketing), compliance staff and staff dealing with new Merchants.

5.2 Confidentiality of Information

WEIPL will strive to uphold the secrecy and confidentiality of merchants and end-user's information and make disclosures only to the relevant authorities and as required under the law. It will treat information collected from merchants for onboarding as confidential and details thereof will not be divulged for cross-selling, or for any other purpose without the express consent of the merchants.

5.3 Money Laundering and Terrorist Financing Risk Assessment:

WEIPL shall carry out assessment of 'Money Laundering (ML) and Terrorist Financing (TF) Risks exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk arising for clients (merchants), countries, or geographic areas, products, services, transactions or delivery channels, etc.

6. Review of Policy

The Company will periodically (once a year) review this Policy in line with the RBI regulations and recommend changes, if necessary, to the Board. Any such updates/ changes to this Policy will be approved by the Board.

Annexure I – KYC documents/information

<table>
<tr><th colspan="2">Customer type: Individuals (Beneficial owner of any legal entity)</th></tr>
<tr><th>Item</th><th>Requirement</th></tr>
<tr><td>Proof of Address & Identity</td><td>a. Certified copy of PAN and
b. Proof of possession of Aadhaar number or any “Officially Valid Document” (OVD) or the equivalent e-document thereof containing the details of identity and address</td></tr>
<tr><td>Company PAN</td><td>Self-attested copy of Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and</td></tr>
<tr><td>Other documents</td><td>Any other documents including in respect of the nature of work/business/profession, the financial status of the customer, or the equivalent e-documents thereof as may be required by the Company</td></tr>
<tr><td colspan="2">List of “Officially Valid Document”
• Passport;
• Driving licence;
• Proof of possession of Aadhaar number;
• Voter's Identity Card issued by the Election Commission of India;
• Job card issued by NREGA duly signed by an officer of the State Government; and
• Letter issued by the National Population Register containing details of name and address.

Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof will be deemed to be OVDs for the limited purpose of proof of address:

• Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
• Property or Municipal tax receipt;
• Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
• Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

Note – The Company will ensure to obtain the OVD with current address updated within three months of receiving the above documents.</td></tr>
</table>

Customer type: Private Limited/OPC/Public Limited	
Item	**Requirement**
Entity Proof	Self-attested copy of COI Self-attested (first 2 and last 2 pages) copy of MOA
Company PAN	Self-attested copy of Company PAN
Board Resolution	Should be signed by at least 2 directors / Company secretary can certify true copy.
GST proof	Self-attested copy of GST certificate / Declaration of non-GST in case GST is not applicable.
Bank details proof	Cancelled cheque / Bank statement with bank seal & sign / Bank letter with seal & sign
Company current address proof	Self-attested copy of Any Utility Bill (not more than 3 months old)
Signatory PAN and address proof	Self-attested copy of PAN Self-attested copy of any Utility Bill (not more than 3 months old) or Aadhar card redacted.
2 directors PAN and address proof	Self-attested copy of PAN Self-attested copy of any Utility Bill (not more than 3 months old) or Aadhar card redacted.

Customer type: Partnership Firms/LLPs	
Item	**Requirement**
Entity Proof	Partnership/LLP agreement deed
Company PAN	Self-attested copy of Company PAN
GST proof	Self-attested copy of GST certificate / Declaration of non-GST in case GST is not applicable.
Bank details proof	Cancelled cheque / Bank statement with bank seal & sign / Bank letter with seal & sign
Company current address proof	Self-attested copy of Any Utility Bill (Electricity / Telephone / Water Bill / Gas bill / Municipal Tax (not more than 3 months old)
Signatory PAN and address proof	Self-attested copy of PAN

	Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.
2 Partners PAN and address proof	Self-attested copy of PAN Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.

Customer type: Sole proprietor	
Item	**Requirement**
Sole Proprietor ID proof	Self-attested copy of PAN card
Entity Proof	Self-attested copy of License under Shops & Establishments Act / Registration for Sales / Service tax / VAT / Excise Registration/ Business License
GST proof	Self-attested copy of GST certificate / Declaration of non-GST in case GST is not applicable.
Bank details proof	Cancelled cheque / Bank statement with bank seal & sign / Bank letter with seal & sign
Company address proof	Self-attested copy of Any Utility Bill (not more than 3 months old) or Bank statement.
Sole Proprietor address proof	Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.

Customer type: Clubs/Societies/Associations	
Item	**Requirement**
Company PAN	Self-attested copy of PAN card
Entity Proof	Registration Certificate or Byelaw or Service Tax Registration
GST proof	Self-attested copy of GST certificate / Declaration of non-GST in case GST is not applicable.
Bank details proof	Cancelled cheque / Bank statement with bank seal & sign / Bank letter with seal & sign
Board Resolution	Should be signed by at least 2 trustees / Company secretary can certify true copy.
Signatory PAN and address proof	Self-attested copy of PAN Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.

2 Trustees PAN and address proof	Self-attested copy of PAN Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.
Company current address proof	Self-attested copy of Any Utility Bill (not more than 3 months old) or Bank statement.

Customer type: Trusts/NGO's	
Item	**Requirement**
Company PAN	Self-attested copy of PAN card
Entity Proof	Trust deed/ Memorandum of Association/Trust registration certificate
GST proof	Self-attested copy of GST certificate / Declaration of non-GST in case GST is not applicable.
Bank details proof	Cancelled cheque / Bank statement with bank seal & sign / Bank letter with seal & sign
Board Resolution	Should be signed by at least 2 trustees / Company secretary can certify true copy.
Signatory PAN and address proof	Self-attested copy of PAN Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card.
2 Trustees PAN and address proof	Self-attested copy of PAN Self-attested copy of Any Utility Bill (not more than 3 months old) or Aadhar card redacted.
Company current address proof	Self-attested copy of Any Utility Bill (not more than 3 months old) or Bank statement.

Annexure-II: Additional documents/information

Category	Certificate
OTC products (Ayurveda, Health supplements)	FSSAI
Herbal	Ayush
Advisory Firm (stock market)	SEBI
Venture Capital Fund Co.	SEBI
Merchant Banking Co.	SEBI
FOREX	FEMA registration, FFMC certificate
NGO	12A, 80G
Finance support for society members	NBFC
Gold	916 Hallmark / BIS
Silver	925 Hall Mark / Related
Insurance	IRDA
Mutual Fund Brokers	AMFI
International Travel /Hotel	IATA
Food Industry	FDA
Internet Service Provider	DOT
SMS/Email/Telemarketing Co.	TRAI
Banks/NBFC's or Money Lending	RBI
Pre-paid/e-wallet, Cash/Smart Card	RBI
Paper/Gift Voucher	RBI
Aircraft Maintenance Related Services	DGCA
Chit Funds	Respective State Govt.
National Housing Finance Co.	NHB
Nidhi Co.	MCA
Gaming	Legal Opinion by the merchant
University/Education Sector	UGC certificate/ICSE/CBSE/AICTE
Branded Products	Dealership Rights
Web host/Domain seller	PCI-DSS
Gemstone/Diamond	GII
Prescription basis medicines	Pharmacy License, Retail/wholesale Drug License, Undertaking of authorized signatory under Drugs & Cosmetics Act – 1940, Declaration (Form 20, Form 21, Form 21B, Form 20B

Above list is indicative

Annexure III: KYC Checklist Grid

Below is the list of all “Business Models” that WEIPL is currently using to onboard Merchants/ Sub-Merchants.

Business Model	**Agreement**	**KYC Checklist**	**Settlement**	Merchant Platform **Compliance**	**Liability**
Direct Merchants	MSA/ME Kit	Complete KYC checks	Merchant	Yes	Merchant
WL partners	With WL Partner only	WL – Complete KYC Sub-ME – Sampling	Partner Nodal/Escrow	WL – No Sub ME - Yes	WL partner
Bank deals	No	MIQ form/Work Order	Partner Nodal/Sub-Merchant	No	Bank
Referral	Both with Partner/ME	Complete KYC checks of ME	Sub-Merchant	Yes	Sub-Merchant
Non WL – Model 1	With Non WL Partner only	Complete KYC checks of ME	Sub-Merchant	Yes	Sub-Merchant
Non WL – Model 2	Tripartite	Complete KYC checks of ME	Sub-Merchant	Yes	SA partner
Cross Border	ME	Complete KYC checks of ME	Merchant	Yes	Merchant
BBPOU (Biller Operating Unit)	Yes, BBPS	Complete KYC checks	Biller	No	No Liability on WEIPL

BO Declaration Draft

BO.docx

Annexure-IV: Red Flags or Key Risk Indicators

The following factors may indicate a higher risk:

- The merchant only requests anonymous or cash-based payment methods
- The merchant is a start-up without an adequate business profile or track record
- The merchant's UBO cannot easily be identified (unusual, unduly complex or opaque ownership structure or because the merchant has issued bearer shares)
- The merchant is reluctant to provide CDD information or appears to avoid (face-to-face) contact
- The merchant has significant business links to high-risk countries
- The merchant does not provide or provides vague reasons for changing service providers
- Merchant's needs may be better served elsewhere
- The merchant's use of the service is unusual (e.g. sends funds to or receives funds from another entity)
- Remittance of monies to countries that are privacy or tax havens or are otherwise considered high-risk countries

The following indicators suggest an increased risk in relation to transactions:

- The merchant's transaction volume is not in line with that expected from the merchant category or based on the information provided at the time of onboarding,
- There are unexpected changes in transaction volume
- The merchant has significant business links to high-risk countries
- The merchant only requests anonymous or cash-based payment methods
- Merchant's transactions stay just below applicable thresholds
- The merchant's use of the service is unusual (sends funds to or receives funds from another entity)
- Transactions are not accompanied by the minimum required information on the payer
- Very high-value transactions which are not in the line of the merchant's business

The following additional factors may indicate a low risk:

- The merchant is a long-standing client whose previous transactions have not given rise to suspicion or concern
- There are no indications that the money laundering and/or terrorist financing risks are increased
- The product or service sought is in line with the merchant's risk profile.

Annexure V: Merchant Platform Compliance Checklist

Merchant's Legal name should be prominently displayed within all the below sections.

About Us

- Merchant's Legal name and profile details.
- Profile should have details such as nature of business and vintage.

Contact Us

- Merchant's Legal name along with complete physical address should be mentioned.
- At least one contact number or Email.

Terms and Conditions Policy

- Terms of service between Merchant and End-users need to be elaborated, specific to the products/services sold through the Merchant Platform.
- Each Merchant must ensure that the End-users is easily able to understand that the Merchant is responsible:
  - for the transaction, including the delivery of the goods (whether physical or digital) or provision of the services that are the subject of the transaction; and
  - for End-users service and dispute resolution, all in accordance with the terms applicable to the transaction
- Applicable laws/jurisdiction needs to be clearly mentioned.

Privacy Policy

- Type of personal information that is collected
- For what purpose the personal information is collected
- With whom the personal information is shared
- Level of security will be applied to the End-user's personal information.
- If card details are collected, then reason and purpose should be stated. Security features with respect to card collection, storage and transmission must be clearly mentioned.

Disclaimer Policy

- Warranties, Limitation of liability and other provisions.

Cancellation & Refund Policy

- Terms of cancellation along with duration needs to be mentioned.
- In case of cancellations from either side, must clearly instruct End-users how refunds can be obtained, what to expect when requesting a refund.
- Refund scenarios along with duration should be mentioned.
- In case of Returns & Exchange (if applicable):
  - Instructions on returning goods, including time frame after delivery
  - Conditions for acceptance of returns/Exchange
  - Consequences of non-acceptance of return

Shipping and Delivery Policy

- Must include shipment terms. Where applicable, different terms should be displayed for domestic and international shipping (assuming different costs and time of delivery are involved). If a consumer can choose different forms of delivery, it must include the involved time frame and costs.