WORLDLINE

Merchant Onboarding and Monitoring Policy

Internal & Restricted

WORLDLINE EPAYMENTS INDIA 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
www.worldline.com

Version Number	:	1.3
Issue Date	:	February 2021

Classification	:	Internal
Process Owner	:	Merchant Underwriting

Review History

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

Approval History

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

ATTENTION:
This document contains information from Worldline EPayments – A Worldline Brand that is confidential and privileged.
The information is intended for the private use of Worldline EPayments – A Worldline Brand only.

Contents

1. Introduction

Worldline ePayments India Private Limited (hereinafter referred as 'WEIPL' or 'Worldline Epayments' or 'the Company') offers a host of payment solutions that includes Payment Aggregator ('PA') services and other ancillary services. The Company is committed towards facilitating PA services to its Merchants.

The Reserve Bank of India ('RBI'), through Guidelines on Regulations of Payment Aggregators and Payment Gateways ('PA Guidelines'), has specified that as the intermediaries are playing an important role in facilitating payments in the online space they should fall under the ambit of regulations and hence decided to regulate in entirety the activities of Payment Aggregators. As part of the PA Guidelines, the entities were mandated to adhere to the merchant onboarding policy. Through this policy, Worldline Epayments wants to establish a comprehensive merchant on-boarding process that will be adhered to while on-boarding merchants on the platform.

2. Defined Terms

2.1. Definitions

Acquiring Bank or Acquirer means a card scheme acquiring organization that partners with WEIPL.

Alternative Payment Method Supplier means a third-party supplier of payment products and/or services.

Board means Board of Directors of the Company

Credit and Risk Department is the department responsible for identifying and assessing new and existing customers. This department consists of four sub-departments: Credit Department, responsible for credit underwriting, Investigations Department, responsible for Customer Due Diligence and AML/CTF and Sanctions compliance, Fraud Department responsible for Fraud prevention and detection and the Transaction Monitoring Department responsible for the detection of money laundering and/or terrorism financing. The Credit and Investigations Departments are responsible for accepting or rejecting new or existing customers and merchant and transaction monitoring.

Note: The term merchant and customer have been used interchangeably throughout the document.

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

Customer due diligence means the collection and analysis of Merchants attributes to determine the risks associated with doing business with them.

Employee means an individual working at all levels and grades within WEIPL, including but not limited to the board of directors, the executive committee, senior managers, officers, and other employees, whether permanent, fixed-term or temporary.

WEIPL means Worldline ePayments India Private Limited or the Company or Worldline.

Worldline Group means Worldline Group S.A.

Merchant means a legal entity(s) with whom the Company has entered into Contract (Merchant Agreement) to provide payments solution services.

Merchant Platform shall mean Website or Mobile Application of the Merchants

Partner Bank means a bank that partners with Worldline Epayments to offer Net banking payment method.

Risk-Based Approach ("RBA") means identifying, assessing and understanding the Money Laundering and Terrorism Financing risks to which the Company is exposed and take measures commensurate to those risks to mitigate them effectively.

Senior Management means members of the Executive Committee of WEIPL.

Ultimate Beneficial Owner (UBO) is any individual who ultimately has (directly or indirectly) interest of 25% or greater in, or who otherwise exercises control over, a merchant.

2.2. Abbreviations

AICTE All India Council for Technical Education

AMFI Association of Mutual Funds in India

AOA Articles of Association

AYUSH Ayurvedic, Yoga and Naturopathy, Unani, Siddha and Homeopathy

BIS Bureau of Indian Standards

CBSE Central Board of Secondary Education

COI Certificate of Incorporation

DGCA Directorate General of Civil Aviation

DOT Department of Telecommunications

DSS Data Security Standards

EDD Enhanced Due Diligence

ERP Enterprise Resource Planning

FFMC Full Fledged Money Changers

FOREX Foreign Exchange

FSSAI Food Safety and Standards Authority of India

GII Gemmological Institute of India

ICSE Indian Certificate of Secondary Education

WEIPL Worldline ePayments India Private Limited

IRDA Insurance Regulatory and Development Authority of India

ITR Income Tax Returns

LLP Limited Liability Partnership

MCA Ministry of Corporate Affairs

MCC Merchant Category Code

MOA Memorandum of Association

MSA Master Services Agreement

NBFC Non-Banking Financial Company

NGO Non-Governmental Organization

NHB National Housing Bank

OTC Over the Counter

OMAF Online Merchant Application Form

PAN Permanent Account Number

PCI Payment Card Industry

RBI Reserve Bank of India

RMS Risk Management System

SA Strategic Alliance

SEBI Securities and Exchange Board of India

TAT Turn Around Time

TRAI Telecom Regulatory Authority of India

UGC University Grants Commission

URL Uniform Resource Locator

VAT Value Added Tax

3. Objective and Applicability

This Merchant Onboarding Policy (this "Policy") is framed by the Company to provide a seamless experience to the merchant. However, at the same time, to ensure that merchants with mala fide intent are not onboarded to the platform.

This policy applies to the Worldline ePayments India Private Limited

The purpose of this policy is to identify, manage, mitigate and when necessary avoid the integrity, reputational and financial risk exposure of WEIPL and Worldline Group when providing payment aggregator services to its customers.

Also, this policy is in concurrent with the Worldline Group Merchant Acceptance and Monitoring Policy.

5. Merchant Acceptance Policy

WEIPL will not do business with illegal, unethical or brand-damaging businesses, or businesses that are deemed to pose an unacceptable risk to the Company. Hence, some merchants will be unacceptable to the Company based on industry, business model or location, even before commencing the underwriting process.

5.1 Acceptance Principles

The Company will not enter in a business relationship with 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
- organised 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

The Company will not conduct business in countries or with entities and individuals which violate applicable sanctions laws and regulations.

The Company will not accept Merchants which may damage the brand or reputation of WEIPL, Worldline Group, its payment partners or Card Associations.

This policy divides merchants into the following groups:

- Unacceptable: Merchants falling within this category may or may not be accepted.
- High Risk: Merchants falling within this category will be first reviewed by the Credit & Risk department by following a specified acceptance procedure

5.2 Unacceptable Industries/ Merchants

Merchants that fall within one of the below categories are unacceptable because their risk is too high and therefore is beyond WEIPL's risk appetite. The risks associated with these industries are related to a variety of reasons including (potential) unethical behaviour, integrity issues, brand-damaging and potential money laundering or terrorist financing.

Following is the list of business models that will never be accepted by WEIPL:

- Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media); escort or prostitution services. Apparatus such as personal massagers/vibrators and sex toys and enhancements.
- Alcohol, which includes Alcohol or alcoholic beverages such as beer, liquor, wine, or champagne.
- Body parts, which includes organs or other body parts – live, cultured/preserved or from a cadaver.
- Bulk marketing tools which include email lists, software, or other products enabling unsolicited email messages (spam).
- Cable TV descramblers and black boxes which include devices intended to obtain cable and satellite signals for free.
- Child pornography in any form.
- 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 the software, video games and other licensed or protected materials, including OEM or bundled software.
- 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.
- Drugs and drug paraphernalia which includes illegal drugs and drug accessories, including herbal drugs including but not limited to salvia and magic mushrooms.
- Drug test circumvention aids which include drug cleansing shakes, urine test additives, and related items.
- Endangered species, which includes plants, animals or other organisms (including product derivatives) in danger of extinction.
- Gaming/gambling which includes lottery tickets, sports bets, poker, memberships/ enrolment in online gambling sites, and related content (Game of luck).
- Government IDs or documents which includes fake IDs, passports, diplomas, and noble titles.
- Hacking and cracking materials which include manuals, how-to guides, information, or equipment enabling illegal access to software, servers, Merchant Platform, 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.
- Offensive goods which include literature, products or other materials that: a) Defame or slander any person or groups of people based on race, ethnicity, national origin, religion, sex, or other factors b) Encourage or incite violent acts c) Promote intolerance or hatred.
- Offensive goods, which includes crime scene photos or items, such as personal belongings, associated with criminals

- Pyrotechnic devices and hazardous materials which include fireworks and related goods; toxic, flammable, and radioactive materials and substances.
- Regulated goods which include airbags; 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.
- Tobacco and cigarettes which includes cigarettes, cigars, chewing tobacco, and related products.
- Traffic devices, which includes radar detectors/ jammers, license plate covers, traffic signal changers, and related products.
- Weapons, which includes firearms, ammunition, knives, brass knuckles, gun parts, and other armaments.
- Bidding/Auction.
- Wholesale currency, which includes discounted currencies or currency, exchanges.
- Live animals or hides/skins/teeth, nails and other parts etc of animals.
- Any intangible goods or services or aggregation/consolidation business.
- Work-at-home information/ freelancers.
- Drop-shipped merchandise.
- Dating services.
- Web-based telephony/ SMS/Text/Facsimile services or Calling Cards. Bandwidth or Data transfer/ allied services. Voice process/knowledge process services excluding Broadband.
- Virtual currencies such as Bitcoins.
- PC support, BPO services and software downloadable (non-copyrighted)
- Electronic Nicotine Delivery Systems (ENDS) including e-cigarettes, Vape, e-Sheesha, e-Hookah, Heat-Not-Burn devices, e-Nicotine Flavoured Hookah, and the like devices that enable nicotine delivery are not sold, manufactured, distributed, traded, imported and advertised in their jurisdictions.
- Any product or service, which is not in compliance with all applicable laws and regulations whether federal, state, both local and international including the laws of India.

5.3 High-Risk Industries

"High-Risk" business models need careful evaluation due to the risky nature of the business, which could cause Worldline Epayment financial losses or compliance issues. Merchants falling within this category will be first evaluated by the Credit & Risk department post conducting thorough due diligence on the merchant.

Following is the list of business models which will be carefully evaluated by WEIPL before accepting them on the platform:

- Multi-Level Marketing schemes or Pyramid / Matrix sites or 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/gambling which includes, memberships/ enrolment in online gambling 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.

5.4 Business Models

5.4.1 Direct Merchants

WEIPL will only onboard entities as its merchants. Individuals will not be onboarded.

The company will only accept merchants that fulfil the following conditions:

- The merchant's name is visible on the Merchant Platform to identify itself by the End-users (cardholder)
- The merchant represents itself as selling the goods or services to the End-users
- It must be clear to the End-users that the merchant is responsible for the transaction:
  - the delivery of the goods (physical or digital) or provision of the services that are the subject of the transaction;
  - providing services to the End-users; and
  - dispute resolution (refunds, chargebacks)

The merchant will sign the Merchant Agreement (and is, therefore, the Merchant of Record).

Also, the merchant must:

- have a permanent location at which the merchant's employees or agents conduct business activity directly related to providing the cardholder with the goods or services purchased in the specific transaction
- assess sales tax/value-added tax/GST on the transaction activity (in places where taxes apply)
- the location is the legal jurisdiction that governs the contractual relationship between the merchant and the cardholder (e.g. terms and conditions).

5.4.2 White label partners

White label partners are entities that facilitate payment gateway services to their merchants (so-called "sub-merchants"), by using our Payment platform. In this relationship, "sub-merchants" will be activated by WEIPL by performing simplified due diligence.

5.4.3 Bank deals

Bank deals will be where Worldline EPayments provides its services directly to the bank's merchants (also merchants for Worldline Epyaments) by performing simplified due diligence.

5.4.4 Resellers

Resellers will be the entities that refer merchants to WEIPL. Through a commission-based (per merchant) referral agreement, WEIPL will accept merchants referred by Resellers after performing standard due diligence.

5.4.5 Strategic Alliance (SA) partner

Strategic Alliance partners will be the entities that refer merchants to WEIPL. Through a commission-based (per transaction) SA partner arrangement, WEIPL will accept merchants referred by SA partner by performing either simple or standard due-diligence.

5.4.6 Aggregators or Payment Facilitators

Aggregators are payment institutions that are or function as a payment facilitator, facilitating payments for their merchants (so-called "sub-merchants").

In an aggregator relationship the Company will carry out payments on behalf of the sub-merchants of its merchant of record, that means there will be an indirect relationship between the Company and the sub-merchants, resulting into the fact that the Company will not Know its End-users, the basic requirement for entering a business relationship.

Due to the high risks related to this indirect relationship the Company will not accept Aggregators/Payment facilitators as a merchant unless it's approved by Senior Management.

5.4.7 Bharat Bill Payment Operating Units – Onboarding of Agent Institution, Agents and Billers

Bharat Bill Payment Operating Units (BBPOUs) are authorised operational units, working in adherence to the standards set by the BBPCU.

The BBPOUs will on-board the billers and aggregators as per standards / rules and will carry out due diligence (as per processes and rules defined in the Standing Operating Procedure); and will ensure the confidentiality and privacy standards.

The BBPOUs will ensure the safety and security of transactions, conduct the verification of biller information and will adhere to the transaction flow standards / rules.

They will also handle the customer grievances and disputes as per set procedures and standards for billers / agents / end-customers. BBPOUs will provide the MIS and Reporting and other services to the billers / aggregators / agents.

Following steps will followed for on-boarding of the billers:

1. Billers will be on-boarded in BBPS by BBPOUs only. BBPOUs will send a formal request for approval to BBPCU for addition of a new biller's name when on-boarded after completion of all formalities and compliance with the standards set by BBPCU for on-boarding of billers.
2. After receiving the approval of BBPCU, the BBPOU will add the entry of the newly on-boarded biller, who will then be listed under the respective BBPOU's profile BBPCU shall issue a unique id for each biller.
3. Same information will be updated to all system participants based on BBPCU authorization/approval. Thereafter the biller will be part of the BBPS and available as ON-US biller for the on-boarding BBPOU and OFF-US biller for other BBPOUs.

The BBPOU should ensure the following while on-boarding billers:

1. The biller is a licensed or authorised entity to raise bills on customers.
2. The bills pertain to the legitimate activities that the biller is engaged in.

3. The biller must a part of the categories authorised by RBI under BBPS.

4. The biller's name does not appear in a negative list of billers whose presence in the BBPS system is considered to be detrimental to the system (as and when such a list is published under BBPS)
5. The biller's name should not appear in the list of banned/ prohibited entities https://www.rbi.org.in/scripts/bs_nbfclist.aspx ; http://mha.nic.in/bo.

6. Relevant information required for the onboarding of biller must be provided by the BBPOUs.

On-boarding of Agent Institutions:

On-boarding of Agent Institutions will be the responsibility of the BBPOUs. Every BBPOU will ensure compliance with the following parameters while on-boarding an agent institution.

Documentation requirements:

Proof of business activity (please refer to the annexure for the list of acceptable documents).

KYC of the key management officials. (Indicative checklist for KYC are listed in the Annexure).

The Agent Institution to be on-boarded:

- Should not be part of blacklist as and when introduced by BBPCU or any other competent authority.
- Should not be bankrupt or insolvent
- Should not have been declared a willful defaulter by any bank or financial institution.
- Should not appear in the list of banned/ prohibited entities https://www.rbi.org.in/scripts/bs_nbfclist.aspx ; http://mha.nic.in/bo

It must be ensured that the volume and amount of bill payments to be handled by the Agent Institution are commensurate with the net worth and capacity of the Agent Institution.

It is of utmost importance that the Agent Institution and Agents appointed by the Agent Institution discharge their fiduciary obligations in regard to payments collected from the customers promptly and without fail. Therefore, the BBPOUs must have in place suitable arrangement, processes and risk control mechanism to ensure that there is no default or delay in effective transfer of moneys collected from the customers to BBPOU. In any case, BBPOU shall be fully responsible for paying the monies collected from customers by Agent Institution and Agents enrolled by the Agent Institution to the Billers in case of ON-US transactions and to the default BBPOUs of Billers through the Clearing and Settlement mechanism for OFF-US transactions.

BBPOU may directly or through a reputed third party assess the prospective Agent Institution's infrastructure to ensure that it is capable of complying with various BBPS requirements, Procedural Guidelines and standards.

BBPOUs must ensure that the requisite infrastructure and contractual commitment for protecting the privacy and confidentiality of sensitive customers data (bank details, passwords, card details, PIN etc.) in compliance with the industry standards as applicable, such as ISO/IEC 27001, PCI-DSS and provisions of the Information Technology Act (as amended from time to time) are in place before commencement of operations.

In addition to the above, the BBPOU officials must undertake a visit to the agent institution to satisfy themselves about the authenticity and credibility of the information provided by institution to be on-boarded.

There should be a proper contractual agreement between the BBPOU and the Agent Institution, including undertaking by the Agent Institution for compliance of the BBPS Procedural Guidelines, Operational Guidelines, guidelines on BBPS brand compliance and applicable standards by the Agent Institution as well as by the Agents on-boarded by them. The contractual arrangement must incorporate provisions which empower BBPCU and BBPOU to delist the Agent Institution and / or Agents in case of serious or persistent violations, defaults, non-compliance, frauds, frequent customer complaints and serious misdemeanor, etc.

The BBPOUs should have a Board approved policy for on-boarding Agent Institutions and Agents, detailing inter-alia process for compliance with the standards prescribed above.

Relevant information required for the onboarding of Agent Institutions must be provided by the BBPOUs

Indicative Requirement of KYC Documents for Agent Institutions & Agents.

KYC Documents Required			
Sole Proprietor Firms	**Partnership Firms**	**Limited Liability Partnership**	**Companies**
	one copy of each	one copy each	one copy each
Proof of Business /Activity (any two documents as per the table)	Registration Certificate.	Certificate of Incorporation (COI),LLP Agreement	Certificate of Incorporation (COI), Memorandum of Association, Articles of Association
Official valid documents (OVDs) of the Proprietor/ Individual	Partnership Deed	Address Proof in the name of LLP if different from COI	Board Resolution
	Official valid documents of Authorised Signatories/ Partners	Official valid documents of Authorised Signatories	Official valid documents of Signatories authorized to transaction on its behalf
		PAN No. of LLP	List of Directors

	Documents Accepted As Business Activity /Existence/ Proof Of The Firm
	Shops and Establishment Certificate
	Registration Certificate
	Sales Tax/Excise/ VAT Registration Certificate
	Sales Tax and Income tax returns
	CST VAT Certificate
	Latest Income Tax Return/Assessment Order with computation having firm name along with acknowledgment from Income Tax Dept.
	License /Certificate issued by any professional body incorporated under a statue.

	Latest utility bill (water/electricity/landline telephone) in the name of the firm (address proof can be used as existence proof for proprietor)

	Officially valid documents of authorised signatories for identity and address proof
1	Passport
2	PAN Card
3	Driving License
4	Voter ID issued by the Election Commission
5	Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.
6	Job card issued by NREGA duly signed by an officer of the State Government,

In the absence of any of the six OVDs, BBPOUs may adopt a "Simplified procedure" means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by them.
Following documents shall be deemed to be OVD for verifying the identity of the above customers;

1. Identity card with applicant's photograph issued by Central/ State government departments, statutory/ regulatory authorities, Public sector undertakings, Scheduled commercial banks, and Public financial institutions;
2. Letter issued by a Gazetted officer, with a duly attested photograph of the person.

In addition to the above any of the following documents are to be considered as OVDs for the verifying the proof of address:

1. Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
2. Property or Municipal tax receipt not more than 2 month old.
3. Bank account or Post Office savings bank account statement.
4. Pension or family Pension Payment Orders (PPOs) issued to retired employees by government departments or Public sector undertakings, if they contain the address.
5. Letter of allotment of accommodation from employer issued by State or Central government departments, statutory or regulatory bodies, and public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation.
6. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.

6. Underwriting

Underwriting will be performed by the WEIPL's Credit and Risk Departments, whereby the Investigations Department will be responsible for Customer Due Diligence, Fraud and Transaction Monitoring Departments will be responsible for setting an expected transaction pattern, and the Credit

Department will be responsible for the Credit assessment. Based on the outcome of the business model study of a merchant it will be decided whether a merchant will be accepted, rejected or additional information will be requested for further understanding the details of the merchant.

For Customer Due Diligence and Screening, the requisite details have been captured in the KYC/AML/CFT policy document.

6.1 Merchant Platform Compliance

The objective of Merchant Platform compliance is to identify the Sector (MCC) of the merchant by verifying the Merchant Platform by obtaining the URL and other details. Once the merchant's industry compatible and MCC is assigned, then it's important to review Merchant Platform thoroughly to ensure the products/services sold are reasonable and all the relevant T&C's, policies are made available for the End-users to review before purchasing.

Below are some of the parameters which will be considered while reviewing the Merchant Platform:

a. To ascertain that the Merchant Platform is LIVE. Merchant Platform with Test/Beta versions will not be permitted.
b. Redirection of the website is not allowed in general, unless it's a Booking engine, ERP provider or if there is a valid justification.

Below T&C's should be available on the Merchant Platform for which PA service is needed:

- About Us (Company Profile)
- Terms & Conditions Policy
- Disclaimer Policy
- Privacy Policy
- Cancellation & Refund Policy (Returns & Exchange in case of E-commerce)
- Shipping & Delivery Policy
- Contact us details
- Brief Description of Products / Services with INR Pricing
- Process flow of Merchant Platform (Till payment page)

Detailed checklist to be validated is listed in **Annexure I**.

6.2 PCI-DSS/PA-DSS

At the time of onboarding, Risk team will verify the Merchant Platform to find out if the merchant is collecting card details on Merchant Platform. In case the merchant is collecting Card details then the following checks need to be conducted:

- Valid SAQ (level 2, 3, 4) or ROC (level 1)
  - Correct version
  - Merchant of record's legal entity name
  - Status compliant
  - Signed and dated by merchant (SAQ) or by QSA (ROC)

- Valid for 1 year after the signature

The above details will be validated by the InfoSec team to ensure that merchant is having necessary certification to collect card details on Merchant Platform.

Merchant could make use of any vendor (PCI recognized) of their choice to do PCI assessment and produce us the relevant documents for Information Security team to validate the same or we could assist them with a vendor to perform PCI assessment.

Similarly, PA-DSS certificate would be collected, wherever applicable from the partner by Risk team and it'll be validated by the InfoSec team.

6.3 Credit Review

The Credit Department will be responsible for the credit review of the merchant and will assess the credit risk by quantifying the credit risk exposure, performing a credit assessment and determining the underwriting conditions.

Credit assessment will focus on the merchant's short-term risk of default/insolvency. Detailed policies & procedures will be covered in the Risk Policy document.

6.4 Risk assessment

The outcome of the customer due diligence and the credit review process will be combined to arrive at risk assessment of the merchant. The Credit and Risk Department will accept or reject a merchant based on the outcome of the risk assessment.

The risk assessment will include:

- Integrity risk: risk of money laundering, terrorism financing or other (financial) crimes that have a potential or reputational, legal and/or financial risk.
- Credit risk
- Expected transaction pattern

6.5 Acceptance/Decline

After the Credit and Risk Department will finish the underwriting and complete the risk assessment merchant acceptance process will be initiated whereby, based on the risk profile allocated to a merchant, a decision will be taken about whether to enter in a relationship with the merchant or not.

Before WEIPL will onboard a merchant to a specific Acquirer or Partner bank, the Alliance Ops department will verify with the acquirer/Partner bank on specific unqualified lists whether the acquirer will be willing to onboard the merchant on its platform.

Both the Credit Department and Risk Department will have an acceptance matrix in place determining the authority level required for merchant acceptance decisions.

Merchants will only be accepted after the drawing up of a complete risk profile and an expected transaction pattern.

7. Review and Monitoring

Company will undertake on-going due diligence of existing customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

The Credit and Risk Department will responsible for performing the continuous monitoring and periodical review of merchants.

7.1 Review

A review will include updating and requesting outstanding merchant information and assessing whether the allocated risk profile and the expected transaction pattern are still valid.

7.1.1 Change requests

Merchant forms will be collected for any changes in the existing details for the following changes:

- Addition of new payment methods
- Addition of new merchant ID (Eg: New product/Line of business)
- Addition of new LID
- URL change
- Merchant details change
- Pricing change
- Bank details change

For all such change requests, merchant consent will be obtained in the form of Signatory confirmation along with supporting documents.

7.2 Monitoring

The intensity of monitoring will depend on the merchant's risk category.

For low and medium risk merchants only unexpected large changes in transaction volumes will require additional attention. While high-risk merchants require increased monitoring meaning that all large transactions that are not standard for the merchant will be reviewed and investigated. Also, fraudulent transactions will be monitored and investigated in accordance with the Fraud policy of the firm.

7.2.1 Merchant Platform monitoring

All merchant-URLs will be monitored continuously on possible violations due to prohibited or reputation harming content.

- This activity will be carried out using an automated web crawling tool. Certain checks will be performed every month to ensure Merchant Platform content is compliant with the norms.
- The tool will scan every Merchant Platform on the following parameters.
    - Content Violation – Check for any banned/restricted or illegal product/services being marketed by the Merchant.
    - Reputation Scan – Checks across various global consumer redressal forums for any complaints of any nature registered against the Company.
    - Merchant Platform Compliance – Checks for any inactive/dead sites, website redirections, violations of Schemes/Regulatory bodies/Banking Channels guidelines.
    - Transaction Laundering – Check if the approved merchant has started accepting transactions from other than the approved website/URL.

7.2.2 Transaction fraud monitoring

Fraud monitoring is mandatory for all merchants. Based on the Merchant profile and the payment methods enabled, Risk Department will decide whether the merchant must use WEIPL Fraud tool or whether its own fraud prevention suffices. The Company has established board approved Fraud Policy for ongoing monitoring of frauds and implementation of adequate mitigation measures for such identified potential frauds.

7.2.3 Credit monitoring

When the Company is notified of adverse media or other alerts (changes to the business model, etc.) relating to its merchants, an investigation will take place to determine whether these alerts are reasonable and whether this impact the current merchant risk rating.

If the merchant's risk rating could be impacted, a full review must be conducted, and a new risk assessment must be performed.

- Each Merchant must undergo credit assessment every month, taking the following factors into consideration
    - Merchant sector
    - Annual volume
    - Historical CB rate
    - Historical Refund rate
    - Existing Risk rating
- Once the financial exposure is calculated as per the credit risk policies
    - Wherever needed, necessary securities (Delayed settlement, rolling reserve, Fixed deposit, Bank guarantee etc.,) must be collected.
    - As per the prescribed Exposure limits, it must go through Credit Manager/Director Risk/Local CRC/Global CRC approval.

- The same procedure is carried out for all merchants as well periodically to estimate overall Credit Exposure of the organization and take necessary precautionary measures.

The objective of doing Credit monitoring is to ensure Chargeback to Sales (CTS) ratio is kept at a minimum thereby reducing credit losses for WEIPL.

8. Remittance

8.1 Remittance Conditions

For WEIPL merchants, Remittance will be allowed only to the following type of accounts:

- Current account
- Cash credit account
- Nodal/Escrow account

Remittance account must be in the Legal entity name of the merchant registered with WEIPL.

Remittance to “Savings” account is not allowed for merchants, except for the below entities:

- Government
- Trusts
- Associations
- Societies
- Clubs
- NGOs
- Hospitals
- Educational and research institutions
- Section 25 companies

In the case of Payment aggregators and White label partners, the remittance will be allowed only to a Nodal/Escrow account.

8.2 Third-Party Remittance

Third-Party Remittance means that the collected payments will be distributed to another party other than the merchant of record. Potential risks associated with Third-Party Remittance will be:

- Compliance & Fraud risk: money laundering, terrorism financing risks, and other (financial) crimes, including sanctions compliance and tax evasion as well as to avoid to compliance with regulations which apply to their business or operations by redirecting the funds to another party (regardless in the same country or abroad).
- Credit risk: liability of WEIPL in case of liquidation of the merchant.

Third-party remittance will only be accepted in exceptional circumstances, provided both merchant and third-party have bank accounts in India.

8.2.1 Acceptable Parties for Third-Party Remittance

Third-Party remittance will be permitted in the following cases:

- **Subsidiaries and Affiliates** (Merchant of record must have substantive control of the third party)
- **Framework parties**
- **Fulfilment companies**
- **Money Services Businesses**

8.2.2 Requirements

The below requirements will exist to minimize the risks related to Third Party Remittance:

- Required documentation
    - Third-party legal entity name.
    - Bank details proof of third-party – Cancelled cheque/Bank statement/Bank letter.
    - Letter from the merchant and third party on merchant letterhead, including
        - Reasons for requesting third party remittance
        - Bank details of third-party.
        - Signatures of authorized representatives from both merchant side and third party along with respective company seal.
        - Indemnifying WEIPL for any liability arising out of the arrangement.
- The investigations manager will verify the information provided by the merchant and must assess if there is a legitimate business reason to allow for this exception. If there is no legitimate business reason the request must be rejected.

8.2.3 Approval process

A Third Party Remittance request will be sent in writing to the Investigations department and will be reviewed by the Investigation Manager and their opinion and recommendation will be based on the standard process.

The final approval for Third-Party Remittance will be given only by Director Risk. Such approval always will be recorded in writing.

9. Closing and/or Termination

To close a Merchant, an Account ID, a Payment Method and a Payment Product where:

1. The merchant will decide to terminate the agreement, the account-ID, a payment method or a payment product

- Merchant will send deactivation form duly signed and stamped to Worldlines EPayments.
- Finance team will validate if there are any dues.
- Chargeback team will validate if there are any outstanding/expected chargebacks.
- Risk team will initiate the process through Prod Team to disable payment methods.

2. WEIPL will decide to terminate the agreement with a merchant, an account-ID, a payment method or a payment product for commercial and/or risk reasons.

- The team which received the request will inform the Business team about the same and get their consent if needed.
- Initiate formal notice to the merchant through the Legal department, as per terms agreed in the merchant agreement.

In the case that a merchant is terminated based on integrity reasons, Management will be informed.

10. Process of Delisting of Billers in BBPS

BBPOU may delist a biller on valid and justifiable grounds. Illustratively, a BBPOU may delist a biller, inter-alia, for any of the following reasons:

1. In case of breach of BBPS guidelines
2. In case of agreement failure between BBPOU & billers
3. In case the biller company declares Bankruptcy
4. In case the biller has indulged in fraudulent practices in billing or collection
5. Any unforeseen circumstance or contingency that compromises or jeopardizes the system.

For any delisting of biller, BBPOU will send a formal intimation/ advice to BBPCU as soon as the event necessitating delisting occurs but in no case later than 30 days.

The delisting will be effective once BBPOU removes the entry of the biller upon receiving BBPCU approval and thereafter the biller will no longer be listed in the respective BBPOU's section. In case a biller has relationship with multiple BBPOUs, the delisting will be effective only for the BBPOU that undertakes the process of delisting biller's entry.

Any delisting application submitted by the Biller through the respective BBPOU will be finally accepted by BBPCU subject to settlement of all outstanding dues and liabilities arising out of complaints/disputes raised on the Biller.

BBPCU may suo-moto require BBPOUs to delist a biller if the biller's continuation in the system is considered to be detrimental to the BBPS system and customers. In such a case the biller will cease to be a part of the BBPS.

11. Waivers

Waivers will only be granted under exceptional circumstances that justify the need for a waiver. A permanent waiver or delayed delivery may be granted on the condition that the customer due diligence can be completed as a result of a complete risk assessment. The department providing the waiver may set additional requirements. These waivers are internal only, that means Merchant Partners will be required to submit the documentation at a later stage.

Document	**Delayed waiver possible**	**Approval Authority – Delayed waiver**	**Permanent waiver possible**	**Approval Authority – Permanent waiver**
OMAF	No	None	No	None
PCI DSS Documentation	Yes	IT head or Company director	No	None
Merchant Agreement	Yes	Legal Head or Company director	No	None
Board Resolution	Yes	Director Risk or Company director	No	None
Bank details proof	No	None	No	None
KYC (Other than BR)	Yes	Director Risk	No	None
Merchant Platform compliance	Yes	Director Risk	Yes	Director Risk
Financial statements	Yes	Credit Manager or Director Risk	Yes	Director Risk
Third-party remittance documentation	No	None	No	None

Any waivers sought by the Business team and provided by the Approval Authority will be recorded over an email and will be stored for later reference and Audit purposes. All such exceptions will be tracked by the Investigations department and maintained as a separate file.

12. Policy Review

The Board of Worldline ePayments India Private Limited will periodically review this Policy and take steps to address any deficiencies in it or in its compliance where required and appropriate. The Board will review the Policy at least once a year.

Annexure I: 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.
- The 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.