SMART PAYMENT SOLUTIONS PRIVATE LIMITED

KNOW YOUR CUSTOMER (KYC) POLICY

Version 2.3

Version control

Date	Version no.	Name of the author	Reviewer
25 Nov.2013	*1.0*	*Mr. Piyush Sharma*	*Mr. Preeti Sharma*
01 Sept.2015	*1.1*	*Mr. Arpit Aggarwal*	*Mr. Praveen Dhabhai*
19 Mar.2018	*1.3*	*Mr. Arpit Aggarwal*	*Mr. Praveen Dhabhai*
22 Nov.2018	*1.4*	*Mr. Arpit Aggarwal*	*Mr. Praveen Dhabhai*
13 Mar 2019	*1.5*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
01 June 2019	*1.6*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
11 Mar 2020	*1.7*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
16 Feb 2021	*1.8*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
17 Mar 2022	*1.9*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
30 Mar 2023	*2.0*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
22 Mar 2024	*2.1*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
18 Nov 2024	*2.2*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
13 Jan 2025	*2.3*	*Mr. Ankit Ahluwalia*	*Mr. Praveen Dhabhai*
Approved by the Director, Mr. Naresh Chandra Mangal			

Index

Chapter – I

INTRODUCTION

1.1. OBJECTIVE

The objective of **KNOW YOUR CUSTOMER (KYC)** guidelines is to prevent semi closed prepaid instruments issuers from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable entities to know/understand their customers and their financial dealings better, which in turn help them, manage their risks prudently.

Sound KYC policies and procedures not only contribute to a SPSPL's overall safety and soundness; they also protect the integrity of the entitling system by reducing the likelihood of unlawful activities.

It is important that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of services to general public, especially to those, who are financially or socially disadvantaged.

1.2. DEFINITION OF A CUSTOMER

For the purpose of KYC policy, a Customer may be defined as:

"Individuals who acquire pre-paid payment instruments for purchase of goods and services."

1.3. SPSPL's KYC policy includes the following key elements:

1. *Customer Acceptance Policy*
2. *Customer Identification Procedures*
3. *Risk management*
4. *Internal Control Systems*
5. *Record Keeping*

SPSPL will conduct regular assessments to identify and mitigate risks related to money laundering (ML) and terrorist financing (TF) for its clients, products, services, transactions, countries, or delivery channels. The risk assessment will consider all relevant factors, including sector-specific vulnerabilities shared by regulators.

The risk assessment will be documented and aligned with the company's size, geographical presence, and complexity. The frequency of the assessment will be determined by the Board or an authorized committee, with at least an annual review. The outcome will be presented to the Board or its committee and made available to relevant authorities and self-regulatory bodies.

Chapter – II

CUSTOMER ACCEPTANCE POLICY (CAP)

As per RBI guidelines the SPSPL should develop a Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy enumerates explicit guidelines on the following aspects of customer relationship with the Company.

1. No electronic or physical card be issued in anonymous or fictitious/ benami name(s);

2. Not to open an account where the SPSPL is unable to verify the identity and /or obtain documents required as per the policy due to non-cooperation of the customer or non-reliability of the data/information furnished to the SPSPL.

3. It may, however, be necessary to have suitable built in safeguards to avoid multiple issuance of card to same customer.

Adoption of customer acceptance policy and its implementation shall not become too restrictive, which result in denial of Basic facility to the members of the general public, especially to those, who are financially or socially disadvantaged.

Chapter – III

3.1. Customer Identification Procedure (CIP)

Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the Officially Valid Documents (OVDs).

SPSPL need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of SPSPL relationship.

Being satisfied means that the SPSPL must be able to confirm the details of the customer, with various verification procedures as per the category of card and satisfy the competent authorities that due diligence was observed in compliance with the extant guidelines in place.

Customer Identification:

The **objectives** of the KYC framework should be to ensure appropriate customer identification.

SPSPL should obtain all information necessary to establish the identity/legal existence of each new customer

For KYC wallet

- Required a one ID proof from mentioned document
- Required One Address proof
- Pan card or Form 60 if customer does not have a pan card.
- Passport Size Photograph

For Minimum detail wallet

- Name
- Contact Number
- Valid ID proof Number

3.2. KYC Norms according to Customer Type

As per the directive issued under **section 18, of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007)** read with "**Issuance and Operation of Pre-paid Payment Instruments in India (Reserve Bank) Directions, 2009"** and amended policy guidelines issued by RBI time to time ,Semi-closed system prepaid payment instruments can be issued up to Rs.10,000/- by accepting minimum KYC details of the customer provided the amount outstanding at any point of time does not exceed Rs 10,000/- and the total value of reloads during any given month also does not exceed Rs 10,000/-. These can be issued only in electronic form.

Accordingly, SPSPL is to obtain the following detail, which are considered as minimum details, and will be considered mandatory for this category.

1) Name
2) Contact Number
3) Valid ID proof number

Semi-closed system prepaid payment instruments can be issued up to Rs.2,00,000/- with full KYC and can be reloadable in nature.

Accordingly, SPSPL is to obtain all necessary information to establish identity and legal existence of each and new customer, based preferably on disclosures by customers themselves and OSV (originals seen & verified) authentication is performed by SPSPL employees, or its Parent company employees and its authorized network.

Easy means of establishing identity would be documents such as passport, driving license, etc.

Document from each of the under noted for a photo ID and proof of residence.

1.	Election ID Card
2.	Passport
3.	Aadhar Card
4.	Pan Card
5.	Govt./Defence ID Card
6.	Driving License
7.	Electricity Bill
8.	Telephone Bill
9.	Bank Statement/Passbook

While the above set of documents should normally suffice to establish both the identity and the correct address of the applicant, wherever this is not so (e.g. PAN Card may not provide proof of address) applicants to be asked to give additional documents.

Apart from above document we will obtain the Pan card no or Form 60 as per the KCYC guidelines.

In case of Bank Statement/Passbook, we are obtaining 1st page of Passbook including address with Bank's official stamp.

3.3. Updation / Periodic Updation of KYC

SPSPL is required to establish a framework for ensuring that the Know Your Customer (KYC) information of customers is periodically updated based on a risk-based approach. This ensures compliance with regulatory requirements and mitigates risks associated with customer identification and due diligence.

Frequency of KYC Updates:

- **High-Risk Customers:** Every 2 years.
- **Medium-Risk Customers:** Every 8 years.
- **Low-Risk Customers:** Every 10 years.

Accordingly, SPSPL is to obtain the detail, which are considered as minimum details, and will be considered mandatory for this categories.

Chapter – IV

Risk Management

An effective KYC programme should be put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the SPSPL for ensuring that the policies and procedures are implemented effectively.

The nature and extent of due diligence will depend on the risk perceived by the SPSPL. However, while preparing customer profile SPSPL should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

SPSPL's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the SPSPL's own policies and procedures, including legal and regulatory requirements. It should be ensured that the audit machinery is staffed adequately with individuals who are well versed in such policies and procedures.

Internal Inspectors should specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard.

Risk Categorization of Customers

We will categories the customer as per their usage in the risk category & monitor the same accordingly. The risk categorization of a customer shall remain confidential.

Usage per month	Risk category
Below Rs. 10 K	Low
Rs. 10 K to Rs.25 K	Medium
Above 25 K	High

Principles for Risk Categorization: The company will consider the following parameters for the risk categorization of customers: verification of identity documents and use of online or authorized services to confirm authenticity; evaluation of the customer's financial background and social standing; analysis of the customer's line of business and associated risks; assessment of the customer's location and risks associated with transactions conducted in specific regions or jurisdictions; identification of risks related to the products or services availed by the customer; consideration of the methods used for delivering products or services (e.g., online, offline); and monitoring transactions such as cash, cheque, wire transfers, and forex transactions.

Chapter – V &
Chapter – VI

Chapter- V

Policy towards Reporting Obligation under AML Compliance:

In terms of the Rules notified under Prevention of Money Laundering Act, 2002 (PMLA) certain obligations were cast on banking companies with regard to reporting of certain transactions. The RBI has issued circular No DBOD.NO.AML.BC.63 /14.01.001/2005-06 dated February 15, 2006 and DBOD.AML.BC. No. 85/ 14.01.001 / 2007-08 dated May 22, 2008, detailing the obligation of banks in terms of the Rules notified under PMLA. According to it, every banking company, financial institution and intermediary shall –

Nomination of Designated Director: Designated Director" means **a person designated by the reporting entity (bank, financial institution etc.) to ensure overall compliance** with the obligations imposed under chapter IV of the Act and the Rules and includes :-
i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
ii) the managing partner if the reporting entity is a partnership firm,
iii) the proprietor if the reporting entity is a proprietorship concern,
iv) the managing trustee if the reporting entity is a trust,
v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, **and**
vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation *- For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 1956 (1 of 1956).*
Policy cum Guidelines on KYC, AML & CFT-Obligations of Bank under PMLA Page 57
In addition, it shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions referred to in Rule 3 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, through submission of CTR, NTR, CWTR, CCR & STR to FIU-IND.

For the above purpose & as per the Recent KYC guidelines Requirement, Mr**. Praveen Dhabhai** has been appoint the Designated director for the KYC related issue & Compliances.

Appointment of Principal Officer:

As directed in PMLA, Bank should appoint a senior management officer to be designated as Principal Officer. Bank should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism Further, the role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to FIU-IND. With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

For the above purpose & as per the Recent KYC guidelines , Mr. Ankit Ahluwalia has been appoint the Principal officer

Chapter- VI

Record Keeping

SPSPL should prepare and maintain documentation on their customer relationships and transactions to meet the requirements of relevant laws and regulations, to enable any transaction effected through them to be reconstructed.

In the case of wire transfer transactions, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the account.

All financial transactions records are to be retained at least for 10 years after the transaction has taken place and to be made available for scrutiny of Law enforcing agencies, Audit functionaries as well as Regulators as and when required.

Chapter – VII

Centralised KYC

The CKYCR rollout has been extended to Smart Payments. For LEs that are opened on or after April 1, 2021, the regulated entities are required to upload the KYC details of LEs as per the prescribed format. Accounts opened prior to this date are to be uploaded onto CKYCR during the periodic updation or earlier when the updated KYC information is obtained/received from the Legal Entity

2. For individuals, KYC data prior to January 1, 2017, is to be uploaded at the time of periodic updation or earlier if certain specific information is obtained/received from the individual.

3. In case a KYC Identifier is being provided by the customer with an explicit consent to download records from CKYCR, REs shall retrieve KYC information from CKYCR and ask for additional information from the customer only under specific circumstances involving change in customer information or additional verification of customer data.

4. KYC Identifier to be communicated to the individual/ LE once the same is generated by CKYCR

General Guidelines

Payworld money has established an effective KYC programme by approving appropriate systems and procedures. It covers proper management oversight, systems and controls, segregation of duties and other related matters. Responsibility is explicitly allocated within the org for ensuring that the bank's policies and procedures are implemented effectively. Payworld's policies are in place for effectively managing and mitigating risks adopting a risk-based approach. Internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures .Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard is put up before the Audit Committee of the Board on quarterly intervals.

Roles & responsibilities of payworld's officers & staff:

Payworld officers/employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. They should not knowingly provide advice or other assistance to individuals who are indulging in laundering activities. Bank officers/employees who suspect any sort of money-laundering activities in course of banking business should refer the matter to appropriate authority immediately. Bank officers/employees should not indulge in unnecessary dialogue or provide unwanted guidance to the customers / intended customers to avoid dispute of any kind in future. *Policy cum Guidelines on KYC, AML & CFT-Obligations of Bank under PMLA* Page 88 Failure to adhere to KYC / Money Laundering policies / procedures may subject bank employees to appropriate disciplinary action or such penal actions and penalties that may be stipulated under any law or regulatory directive. In general terms there are **FIVE** golden rules to be followed:

1. You **MUST NOT** assist anyone whom you know or suspect to be laundering money that has been derived from any crime.

2. You **MUST** report any transaction which you suspect might be related to drugs, terrorism or other serious crimes.

3. You **MUST NOT** reveal in any way to anyone that a customer is being investigated or that they have been the subject of a report except to your Manager and controlling authorities.

4. You **MUST NOT** go overboard in seeking information for KYC compliance and thereby invading into client's privacy, to avoid intrusion.

5. You **MUST NOT** divulge customer information for cross selling or any other like purposes.

Duties/ responsibilities of officers/staff:

The following duties/ responsibilities arising to the officers/ staff out of the KYC guidelines.

Staff/Officer/ Manager vested with the authority to open new wallets

- To interview the potential customers intending to open account.
- To verify the introductory reference/ customer profile.
- To ensure not to open account in the names of terrorist/banned organisations.
- To adhere with the provisions of Foreign Contribution Regulation Act (FCRA), 1976.
- To comply with the guidelines issued by the Bank from time to time in respect of opening and
- Conduct of account.
- Manager To scrutinize and satisfy himself the information furnished in the Account opening form/ customer Profile/ threshold limit are in strict compliance with KYC Guidelines before authorizing Opening of account.

Nodal Officers

The indicative roles and responsibilities of the Nodal Officers are appended:-

- To co-ordinate all operational issues related to AML & KYC.
- To keep functioning as a 'liaison officer' in between the branches and the controlling offices, and
- to ensure implementation of KYC norms & AML measures
- To keep field functionaries apprise of AML & KYC matters like off-line alert monitoring for picking up suspicious transactions for reporting under STR, proper marking of each account with occupation and activity code.
- To ensure that no account exists with junk/ invalid PAN.
- To monitor newly opened account for at least 2 quarters giving emphasis in high volume & high
- Value transactions.
- Any other issues related to AML & KYC norms.

Evaluation of KYC Guidelines by Internal Audit and Inspection System:
While conducting audit / inspection of the branches / offices should verify compliance of the KYC guidelines and prevention of money laundering at branches and report the cases of deviations, if any, in the report.