Anti-Money Laundering and Countering the Financing of Terrorism (AML & CFT) Localpayment Policy

Contents

1. Overview

Introduction

Localpayment (“LP”),, is the holding company of LP subsidiaries globally and together, is known as the LP Group (“LP GROUP”). LP has oversight on the activities and operations of its subsidiaries under a proprietary software developed by its own software engineers.

Purpose and Scope

The purpose of the Policy is to set out the principles and measures that LP follows to comply with Anti-Money Laundering and Counter Financing of Terrorism (“AML/CFT”) legislation and to identify, mitigate and manage ML/TF risks it faces in the course of its operations.

The Policy is applicable to all LP employees, secondees, contractors and interns. Failure to comply with the Policy may result in disciplinary action, suspension and/or termination of employment. All LP employees have the following responsibilities:

- Comply with AML/CFT policy, program, standards and procedures
- Complete AML/CFT training as required and defined by job role
- Escalate and report suspicious transactions to the AML/CFT Compliance Officer or delegates
- Maintain records in accordance with the record keeping requirements set out in the Policy
- Do not commit an offence of tipping off.

The Policy will be reviewed and/or updated at least once a year to remain in line with the regulatory requirements.

Principles

Senior management of LP is committed to support a culture of compliance by ensuring:

- LP has a robust AML/CFT Program on global as well as subsidiaries-level
- LP works in conjunction with the government and supports the government’s objectives in relation to prevention, detection and control of financial crime including ML and TF
- LP may decide not to provide products or services based upon decisions guided by ML/TF risk appetite, corporate social responsibility, or business efficacy.

Products and Services

LP creates, develops and maintains the payment services platform that allows the launch of payment products within the platform. The products offered by LP can be categorized into 3 groups:[1]

- PAYOUTS - cross-border payments allowing individuals, corporates and financial services clients to make international money transfers at a low cost
- SPEND - card issuing and processing
- PAYINS - global multicurrency accounts allowing corporates to collect and aggregate funds from multiple sources / channels for repatriation or further disbursement.

Payment services offered by LP in the categories of SEND, SPEND, RECEIVE are vulnerable to ML/TF risks. In recognition of these risks, all new designated services or products are subject to a risk assessment by the AML/CFT Compliance Officer prior to its launch.

The current acceptable forms of payments include electronic funds transfer / bank transfers / wire transfers, debit cards, ACH.

LP does not accept cash as a mode of funding transactions / customers' accounts and therefore LP is aware of the Source of funds for every customer's account and transaction.

LP does not engage agents as part of its distribution strategy – customers sign up for LP's services either via website or the onboarding process is facilitated through LP's Business Development Team.

LP's Three Lines of Defense

LP is committed to have an effective "three-line defense model" for AML/CFT which sets three tiers of protection against the various risks posed.

The three lines of defense provides clarity in responsibilities and accountabilities between the three lines and ensures effective independent oversight and assurance activities take place, covering key decisions and processes.

- First line of defense - Business Functions

The business functions are relied upon to identify, measure, monitor and control the AML/CFT risks within their areas of accountability. The business functions are required to apply AML/CFT policies and procedures as they have been laid down as well as to establish effective governance, risk and control frameworks for their business unit to ensure they are compliant with LP's AML/CFT program requirements[2].

[1] SPEND and RECEIVE to be launched in 2020

[2] For example, in relation to issues such as customer identification, transaction monitoring, name screening, funds reconciliation, refunds processing, suspicious reporting, etc.

- Second line of defense - Compliance and Risk & Governance functions

The Compliance and Risk & Governance functions exercise general oversight of all AML/CFT activities within LP including designing policies, conducting trainings, engendering senior management support, monitoring and reviewing the application and effectiveness of policies and controls within the business units, reporting accuracy, regulatory compliance, quality assurance and timely remediation of insufficiencies.

The second line is also responsible for reporting on the compliance and risk profile of LP and ensuring that high/extreme risks, and those beyond LP's risk appetite, all have mitigation plans and that those plans are being executed.

- Third line of defense – Audit/Independent testing and the Compliance Committee

LP ensures that its AML/CFT program is getting audited annually. It is achieved by hiring independent external audit service providers or engaging an internal audit function where appropriate. The audit is aimed at the assessment of the design adequacy and operating effectiveness of LP's AML/CFT controls. The audit provides assurance to the senior management and the Compliance Committee that AML/CFT program is designed and executed to cover LP's risk exposure to ML/TF risks.

Roles and Responsibilities

Senior Management

Senior Management is responsible for the oversight of the following:

- Ensure qualified officers are appointed
- Provide oversight on key control functions development and implementation of the policies, procedures and controls to address key ML/TF risks and enable LP to effectively manage and mitigate these risks.

AML/CFT Compliance Officer

The AML/CFT Compliance Officer is the contact point for receiving and investigating reports of suspicious activities made by staff members, and disclosing them, where applicable, to the relevant authority Key responsibilities:

- Ensure continuous compliance with the obligations to the AML/CFT rules
- Review of the enterprise wide ML/TF risk assessment
- Ensure that risk assessments are up to date
- Contribute and give AML/CFT Compliance advice on new products, projects, delivery channels, etc.
- Oversight of AML/CFT policies, procedures systems and controls to ensure they are operationally adequate and effective to mitigate the ML/TF vulnerabilities LP is exposed to in its normal

course of business

- Liaise and update senior management on AML/CFT issues, any relevant legislative and regulatory update/changes
- Review and approval of the Politically Exposed Persons s handling process
- Provide clear and regular oversight to the Leadership Team and Compliance Officers on AML/CFT compliance matters
- Provide advice and guidance to 1st Line of Defense teams on ML/TF risks
- Ensure that the appropriate AML/CFT training is delivered to all required employees
- Be the point of contact to the supervisory authority and law enforcement agencies
- Identify and report any non-compliance as and when identified
- Ensure LP's adherence to all other relevant and associated regulatory obligations including, but not limited to, recordkeeping obligations
- Investigation and reporting of any confirmed Sanctions matches.

Please refer to the below for the contact details of the AML/CFT Compliance Officer at LP:

c.o@localpayment.com

Policy References

The Policy complements other policies and documents, where applicable, including, but not limited to:

- LP AML/CFT Global Policy
- On-boarding Policies and/or Procedures
- Sanctions Policies and/or Procedures
- Monitoring and Screening Policies and/or Procedures.

2. AML/CFT Program

Risk-Based Approach ("RBA")

The main types of risk that LP may be exposed to include:

- Regulatory risk - risk posed as and when LP does not meet its regulatory obligations under the relevant AML/CFT regulations such as failure to complete reporting obligations, STR, etc.
- Business risk - risk posed as and when LP may be used as a vehicle for ML/TF purposes and illegal activities such as fraud, scams which would damage the LP brand and reputation.
- Financial risk - risk of financial loss incurred through either customer dishonored payments, additional costs incurred to remedy identified customer issues, complaints, regulatory penalties etc.

LP adopts a risk-based approach when managing its exposure to the risks and ensures that the systems and controls it adopts are appropriately aligned with LP's risk appetite.

LP applies resources in accordance with priorities so that the greater risks receive the highest attention.

Enterprise Wide ML/TF Risk Assessment

The foundation of LP's risk-based approach lies in its enterprise wide ML/TF risk assessment. To assess its ML/TF risks exposure LP evaluates risk factors based on the following categories:

- Customers
- Geographies (the countries or jurisdictions LP's customers are from or in and the countries or jurisdictions LP has operations in)
- Products, services, transactions, and delivery channels of LP.

LP keeps a record of the enterprise wide ML/TF risk assessments conducted and updates it periodically.

Customer Factors

Evaluation of ML/TF risks attributable to LP's customers may include assessment of the following factors:

- Extent to which LP's customers pose ML/TF risks
- Extent to which the customer due diligence process is effective
- Extent to which some customers may provide misleading/fraudulent information or documents
- Customers that are outside of LP's risk appetite

- Customers who pose higher ML/TF risks including Politically Exposed Persons engage in ML/TF or other illegal activity via LP
- Volumes and sizes of customers' transactions are not in line with the usual activities and the risk profiles of LP' customers
- Customers may be subject to sanctions.

Geography Factors

Evaluation of ML/TF risks attributable to geography may include assessment of the following factors:

- Customers may transact from and to the countries which pose higher ML/TF risks or subject to sanctions
- Customers may be nationals of the countries which pose higher ML/TF risks or subject to sanctions
- LP may operate from and in the countries which pose higher ML/TF risks.

Products/Services Factors

Evaluation of ML/TF risks attributable to products/services may include assessment of the following factors:

- LP accepts third-party funding for customers' transactions
- Customers request refunds to third-party accounts
- LP accepts cash as a mode of payment for money transfer services (SEND) or as a channel for loading customers' accounts (SPEND and RECEIVE)
- LP uses cash as a channel for pay-outs (SEND)
- LP uses cash withdrawal as a channel for redemption and spending (SPEND and RECEIVE)
- LP processes card payments to restricted type of merchants
- LP processes ATM withdrawals in the countries which pose higher ML/TF risks or subject to sanctions
- LP processes unauthorized card payments.

Delivery/Distribution Channel Factors

Evaluation of ML/TF risks attributable to delivery/distribution may include assessment of the following factors:

- LP offers payment services via web-based applications (website and mobile applications) which entails risks related to non-face-to-face business relations, i.e., the risk of impersonation
- LP appoints agents to offer cross-border money transfer service.

Client Acceptance/Onboarding

LP utilizes the "Know your customer" principle for Client acceptance purposes. Due diligence shall be conducted for all customers prior to account opening.

The level of the due diligence applied during the customer acceptance process is determined by the level of the ML/TF risks attached to different types of customer profiles. LP will only do business with customers who fall within the risk appetite of LP applies three levels of due diligence – Simplified Due Diligence ("SDD"), Standard Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD"). Customer acceptance process at LP consists of two stages – 1) Client identification and due diligence and 2) customer verification and screening.

LP provides payment services to individual, corporate and financial services clients.

Individual Client Onboarding

LP establishes business relations with individual clients who are 18 years or older.

As part of the customer identification and LP collects the following details for individual customers:

- Full name, including any aliases
- Unique identification number
- Residential address
- Date of birth
- Nationality
- Contact information – email address and mobile number

LP applies risk scoring tool for individual customers at the onboarding stage. The risk rating varies from low to restricted. Clients with restricted risk cannot be onboarded. If the initial score appears to be restricted, additional details will be requested from the client to better understand the client's risk profile. Based on the information received from the client, assessment of the risk mitigation factors of the compliance analyst, the initial score may be adjusted from restricted to high after which the individual client can be onboarded.

LP gives individual clients two options of verifying their identity: a) through digital personal data platform such as electronic verification process or by providing additional documents non-electronic verification process.

- Electronic verification process - LP considers Info to be a reliable and independent source for the purposes of verifying the individual customer's name, unique identification number, date of birth, nationality and residential address.
- Non-electronic verification process - as part of the non-electronic verification process, any individual customer can be verified by providing a scanned copy (front and back) of a valid government issued identity card which contains the name, photograph, unique identification number, nationality, date of birth. LP also accepts copies of valid passports, driver's licences, national identity cards as proof of identity documents. In addition, an individual is required to submit a proof of address. Examples of the documents which can be accepted as a proof of address include utility or broadband services bill, bank or credit card statement or government-issued letter. The proof of address must include the customer's residential address and be dated within the last 90 days. PO boxes are not accepted as a proof of address.

Corporate Client Onboarding

As part of the client identification process and LP collects the following details for corporate clients:

- Name
- Unique entity number
- Registered and business addresses (if different)
- Date of incorporation
- Country of incorporation
- Legal form (sole proprietor, private limited, partnership, etc)
- Full name and unique identification number for directors or partners
- Full name, unique identification number, residential address, date of birth, nationality of individuals who are authorized[3] to deal with LP on behalf of corporate customer
- Contact information – email address and mobile number
- Intended use of account
- Industry sector.

[3] Such authorisation is supported either by the position held in the corporate customer (i.e. director) or documentary evidence (i.e. letter of authority or board resolution)

LP may deploy external service providers which provide access to official commercial register information. LP considers the information obtained from the official commercial registers to be reliable and independent source of information and does not require further verification.

Otherwise, LP verifies corporate customers based on the corporate documents as well as the information obtained by the Business Development Team. LP collects the following documents from the corporate clients:

- Business profile issued by the accounting and corporate regulatory authority or an equivalent document for registered companies
- Valid proof of identity as well as acceptable proof of address of individuals who are authorized to deal with LP on behalf of a corporate customer. Where available, individuals who are authorized to deal with LP on behalf of a corporate customer can be verified via an electronic verification process (please refer to electronic verification process for individual customers above)
- Appropriate documentary evidence authorizing certain individuals to deal with LP on behalf of a corporate customer which includes a board resolution or similar authorisation documents.

LP to identify and verify the identity of a Beneficial owner. Any individual who owns directly or indirectly 5 % or more of shares in a corporate clients is considered a Beneficial owner. If no Beneficial owner can be identified based on the documents provided by a corporate client, LP will obtain a declaration from the corporate client stating who is a Beneficial owner. Beneficial owners are subject to identification and verification process which is equivalent to the verification of individual clients stated above. Where available, Beneficial owners can be verified via an electronic verification process (please refer to electronic verification process for individual customers 2.3.1. above).

LP applies risk scoring tool for corporate customers at the onboarding stage. The risk rating varies from low to high.

Financial Services Client Onboarding

Financial services clients (Banks, Payment and E-Money Institutions, etc…) are onboarded based on the principles stated in the Section 2.3.2 of the Policy for corporate clients onboarding. However, there are additional documents which are collected as part of the onboarding process:

- Application form describing major details of the client's business, information about the AML/CFT policies and controls as well as intended use of the services offered by LP
- Financial services licence/registration (where applicable)

- AML/CFT policy or its equivalent (where applicable)
- Additional documents/evidence as may be necessary in proportion to the risk and complexity of the client's business.

LP applies risk scoring tool for financial services clients at the onboarding stage. The risk varies from low to high.

Simplified Customer Due Diligence ("SCDD")

LP may apply simplified customer due diligence to publicly listed banks that are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force.

Enhanced Customer Due Diligence ("EDD")

Where customers are assessed to pose higher ML/TF risks, LP may exercise EDD aimed to highlight the risks which cannot be detected during CDD. Enhanced due diligence may apply to individual, corporate and financial services clients.

EDD may be triggered, but not limited to the following circumstances:

- Individual customer transaction exceeding prescribed amounts on a single transaction basis and/or cumulative over a period
- High or restricted initial onboarding or ongoing risk score
- Involvement of politically exposed persons
- Ongoing customer behavior that results in a modification of the risk ranking based either on periodic customer due diligence or an event trigger.

In order to exercise EDD and depending on the customer type (individual, corporate or financial services) LP may at its discretion request additional information such as proof of source of wealth, inquire on the employment status or relationship with beneficiary, specify countries he/she would like to transfer money to, ask to provide bank statements, copy of lease agreement for business premises, copy of CV/resume for the compliance officer, AML/CFT compliance training material and evidence of employee participation, the most recent internal/external compliance program audit report.

Politically Exposed Persons ("PEPs")

When any individual dealing with LP in a certain capacity (individual customers, directors/partners of corporate customers, individuals who are authorized to deal with LP on behalf of a corporate customer, Beneficial owners) is identified as and confirmed to be a PEP, the individual customer or

corporate customer concerned may be subject to EDD, depending on the risk and influence of the PEP. If the assessed risk exceeds that of LP's acceptance, the relationship may be terminated.

CDD Measures for Non-Face-to-Face Business Relations

Payment and related services are offered by LP via web-based applications (website and mobile applications) which entails risks related to non-face-to-face business relations, i.e. the risk of impersonation. LP may apply the following controls to mitigate these risks:

- Verification through digital corporate and personal data platforms
- Self-portrait digital photograph ("selfie") taken together with the identity document
- Biometric verification solutions including face liveness detection software to prevent presentation attacks
- One-time passwords
- Multi-factor authentication
- Funds reconciliation procedure aimed to match client name with the name of the person who funded the transaction.

Unacceptable Customers and Relationships

The below is the list of LP's unacceptable customers and relationships:

- Customers involved in illegal product or services
- Customers involved in unregulated or unauthorized financial/payment services
- Customers involved in drug related activities, including drug paraphernalia
- Customers under sanctions of the UN, the EU, the US, the UK and other national sanctions regimes
- Customers transacting to/from embargoed countries
- Shell banks and unlicensed financial/payment institutions
- Customers with known or suspected involvement in money laundering, terrorist financing, weapon of mass destruction proliferation, tax evasion or other financial crimes
- Anonymous accounts or account in fictitious name
- Online pharmacies, pseudo-pharmaceuticals, adult industry product and services, trade in endangered/protected animal products
- Weaponry, military and semi-military goods and services manufactures and providers, and related goods.
- Multi-level marketing, pyramid schemes, referral marketing.

- Unregistered charities or nonprofit organizations, and any anonymous payment mechanisms such as crypto-currencies, crowd funding, etc…

Upon approval of the Chief Compliance Officer and Chief Executive Officer, LP may at its discretion allow under exceptional circumstances activity related to this list where is in compliance with the relevant laws and regulations and the business establishes fit for purpose risk mitigation measures.

Ongoing Customer Due Diligence ("OCDD")

LP ensures that the customer information recorded is up-to-date and relevant via ongoing customer due diligence. OCDD is conducted to ensure effective ongoing monitoring and to understand customers' activities as an integral part of the AML/CFT controls. Where suspicious activity has been identified, the AML/CFT Compliance Officer should be notified.

The onboarding risk rating of the customer determines the frequency of the review. The following table denotes the minimum frequency of review:

Risk Category	**Frequency of Review**
Low	3 years
Medium	2 years
High	1 year

To combat ML/TF risks, LP must observe the conduct of the customer's account and scrutinize transactions undertaken to ensure that the transactions are consistent with the expected activity. This may result in the change of the risk rating.

Transaction Monitoring

Transaction monitoring at LP is based on a combination of automated and manual monitoring. Automated monitoring is achieved via a transactions monitoring system, which runs the event triggers on transactions processed by LP in real-time. The system is dynamic, and the event triggers are periodically updated to be in line with the ML/TF risk exposure of LP. The AML/CFT compliance officer is responsible for maintaining on a periodic basis the ongoing validity of system triggers.

In addition to regulatory prohibitions (e.g. sanctions, financial crime), LP maintains a policy of rejecting the following nature and purpose of transactions due to either being unethical or subjected to higher risk:

- Confirmation of payments associated to adult services
- Payments associated with scams
- Transactions associated with terrorism financing and financial crime
- Transactions associated with online gambling
- Transactions to charities (exceptions maybe granted for recognized charities, national event driven emergencies e.g. India Prime Minister relief funds).

The transactions hit by the event triggers are subject to a manual review by LP's Compliance Team. The system triggers are aimed to detect transactions with no visible or lawful purpose, structuring, unusual patterns consistent with certain predicate offences (possible terrorist financing, child exploitation, corruption nexus, etc), transaction activities with nexus to higher risk countries or geographies, hidden relationships between customers or accounts evident though fund flows, other anomalous and unexplained behaviors. The system triggers are set as limits, key words and scenarios. LP also conducts post transaction monitoring analysis on its customers to identify, review and assess suspicious transactions patterns including but not limited to:

- Multiple payments to the same beneficiary from different customers
- Third party funding of transactions
- Large transactions in terms of volume and value
- Payment to beneficiaries with no logical explanation or economic justification.

Reporting Obligations

Suspicious Activity Monitoring

LP monitors transactions and customer activities in line with the LP transaction monitoring procedures. Suspicious matters/transactions may be flagged or identified by all employees of LP. Suspicious matters may be identified at the following points:

- At the time of the customer online registration
- Whilst conversing with the customer about the nature & purpose of his transactions
- Through the Customer identification/verification process
- As part of transaction monitoring exercises.

LP Compliance will adopt the below mentioned principles (not exhaustive) when ascertaining if an activity, transaction or customer give reasonable grounds for suspicion:

- Transaction requested is unusual based on customer's profile
- Transaction does not make economic sense
- High value/ volume account activity
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Customer refusal to provide identification/ supporting documents when requested
- Primary identification documentation provided seems forged or not consistent with the standard format of the issued government identification documents
- Reluctant to provide complete information about nature and purpose of business, anticipated account activity, directors or significant controller of the firm and/ or business location.

Suspicion is a subjective matter and does not require "proof" or "evidence" of ML/TF activities. There is no definitive list of what constitutes suspicious activity. However, the "Know your customer" information that is collated on all customers should enable a build of the customer's risk profile and determine if there has been potential suspicious activity based on this.

Suspicious Transaction Report ("STR") Procedure

All LP staff can raise a suspicion internally. Where a member of staff decides that this is appropriate due to knowledge, suspicion, or reasonable grounds for suspicion, they should as soon as practicable raise the issue with the AML/CFT Compliance Officer for further assessment and action.

When notified of/having identified a suspicion of a ML or TF activity, the AML/ CFT Compliance Officer should:

- Review the detail of any reported/identified suspicion and where necessary seek further information from the staff member or other sources available to the Compliance Department.
- Remind the reporting employee of their responsibility not to tip off the customer

AML/CFT Compliance Officer should make an ultimate decision on the action, including documentation, to be taken on the case:

  - Whether the report should be escalated
  - Whether the report can be de-escalated following a thorough investigation; or
  - Any other measures or controls taken against the customer such as increased monitoring of the customer or temporarily suspension of the account

- When the decision is made, the underlying rationale should be documented.

The AML/CFT Compliance Officer has ultimate responsibility for deciding if the STR should be reported to the regulatory authority or escalated internally. The AML/CFT Compliance Officer may seek guidance from

the Group Chief Compliance Officer while making this decision. Where reporting is required, the AML/CFT Compliance Officer will complete the STR report and submit it to the Suspicious Transaction Reporting Office ("STRO")[4] within 15 business days from the day of escalation to the AML/CFT Compliance Officer. A log of all STRs, including those not filed to the STRO will be maintained by the AML/CFT Compliance Officer.

Tipping Off

The employees of LP are prohibited from notifying the customer or any other persons, or allowing them to understand in any other ways, that information on the monetary operations being performed or transactions being concluded by the customer or on the investigation conducted in their respect has been submitted to the regulatory authority. Please refer to the Section 1.4 of the Policy on the offence which tipping-off carries.

Provision of Information to Relevant Authorities

LP will ensure its compliance with regulations as per the relevant jurisdictions by filing all the required reports within the prescribed period and in the prescribed form e.g., threshold transaction reports, Suspicious Transaction Reports, etc.

AML/ CFT Compliance Officer are responsible for prompt provision of the information in case of the requests from law enforcement agencies.

Compliance with Seizure Orders

As a provider of payment services LP may receive seizure orders issued by law enforcement agencies. The AML/CFT Compliance Officer will work together with the senior management as well as will engage other relevant teams to ensure compliance with the seizure orders, particularly in relation to the freezing and unfreezing of accounts.

Sanctions Compliance

Compliance Obligation

Sanctions may be issued against countries, individuals, corporates or financial services organizations. Given the nature of its business, LP is obliged to comply with sanctions regime of the UN, the EU, the US, the UK and other national sanctions regimes.

LP does not:

- Operate in sanctioned countries
- Process inward and outward payments from and into the sanctioned country
- Establish business relations with the customers based in or linked to a sanctioned country
- Establish business relations with the individual, corporate or financial services clients which are subject to sanctions.

Please refer to Appendix 3 for the list of Prohibited countries.

In order to meet its statutory obligations, LP has implemented systems and controls as a measure to identify prospective (and existing) customers who pose sanctions concerns. As regards to this, LP takes the following steps:

- Undertaking customer due diligence at the onboarding stage to identify sanctions exposure
- Undertaking sanctions screening on an ongoing basis and against the appropriate jurisdictional lists
- Business relations are to be performed in line with the sanctioned and restricted countries requirements.

Screening

LP conducts screening through proprietary and third-party risk intelligence databases to identify any PEPs, state-owned enterprises, individuals or corporates under sanctions, proscribed entities and any other adverse findings which may affect customer onboarding process or transactions processing.

LP screens:

- Names of customers
- Names of individuals who are authorized to deal with LP on behalf of a corporate or financial services client
- Names of directors or partners of a corporate or financial services client
- Names of beneficial owners
- Names of wire transfer originators
- Names of wire transfer beneficiaries

Screening is completed before business relations are established with a customer as well as on each transaction after LP established business relations with a customer. The results of screening and LP's assessment are getting recorded.

Screening is performed against the following lists: EU, UK, US, OFAC, UN

Regulatory Reporting Obligation

All confirmed sanctions matches will be reported by the AML/CFT Compliance Officer to the regulatory authority and STRO.

In the event of a breach to the sanctions policy and, in addition to fulfilling its local reporting obligations, LP will also contact the relevant regulatory authority in whose jurisdiction the event took place. Where there is a conflict, or potential conflict between regulatory obligations and compliance with sanctions policy, immediate escalation must be made to the AML/CFT Compliance Officer for guidance.

Outsourcing

LP are aware of the inherent risk of outsourcing. As such, LP puts in place appropriate controls to monitor the activities of those internal/external outsourced services providers.

The AML/CFT Compliance Officer remains ultimately responsible for outsourced activities including AML/CFT obligations. Currently, LP has few intra-company outsourcing arrangements in place. The AML/CFT Compliance Officer ensures that the intra-company outsourced services providers are duly informed on the AML/CFT obligations as well as AML/CFT trainings.

The AML/CFT Compliance Officer will ensure that proactive monitoring is conducted for outsourced activities which includes regular quality assurance and compliance monitoring activities.

Record Keeping

LP shall maintain and retain all records relevant to its AML/CTF Program and policy including:

- AML/CTF Program and all reviews and addendums to the same
- Transactional records
- Customer identification and verification records
- Audits and compliance reviews
- Suspicious transaction reporting
- Customer account/relationship records
- Compliance reports and other management reports, etc.

Periods of and Measures for the Storage of Information

According to the regulatory requirements all customer records, transaction records, documentation collected from the customer, written or electronic correspondence relating to the business relations with

the customer, reporting filed with the regulator must be kept for a period of at least 5 years following the termination of such business relations.

Employee Due Diligence, Training and Audit

Internal and Independent Review

LP will conduct an independent review of its AML/CTF program on a periodic basis.

Employee Due Diligence

LP will conduct background checks on all new employees.

Employee Training

LP has implemented procedures in order that new and existing staff members are trained on a periodic basis. New joiners must complete an online AML training upon joining. LP will maintain a record of completed training. All employees are made aware of their legal and regulatory duties and requirements. Staff will also receive training whenever there is a regulatory update that affects LP's obligations, or at least once a year.

Review of the AML/CTF Program

The content of the AML/CFT program is appraised periodically for adequacy by the AML/ CFT Compliance Officer or Group Chief Compliance officer who will incorporate changes based on:

- Findings of independent reviews
- Regulatory authority feedback and
- Changes to the AML/CFT regulations.

APPENDIX 1 - Definitions

AML/CFT Program

Anti-money laundering and countering the financing of terrorism ("AML/CFT") program refers to the all the policies, procedures, systems and controls in place for AML/CFT.

Beneficial owner

Any individual who: (a) Ultimately owns or controls (whether through direct or indirect ownership or control) 3% or more of the shares or voting rights of the customer's business; or (b) Otherwise exercises control over the management of the customer's business. There may cases when LP may lower down the threshold that a customer poses higher ML/TF risks.

Customer

Means a person (whether a natural person, legal person or legal arrangement) to whom LP either executes a payment or collects a payment.

Client

Means a person (whether a natural person, legal person or legal arrangement) with whom LP establishes or intends to establish business relations.

Business relations

Means the opening or maintenance of an account (whether a payment account or otherwise) by LP for the purposes of accepting, processing or executing any transaction in the name of a person (whether a natural person, legal person or legal arrangement).

Money laundering ("ML") and terrorist financing ("TF")

ML is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. There are three common stages in the laundering of money, and they frequently involve numerous transactions:

a) Placement – the physical disposal of the cash proceeds of criminal activity into the financial system;
b) Layering – the process of separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and separate the money from its origin;
c) Integration – the return of "laundered" proceeds back into the economy. If the layering process has been successful, the criminal source of the funds will be totally disguised in such a way that they appear to the financial system to be legitimate investment funds.

Criminal activities include but are not limited to drug trafficking, tax evasion, illegal gambling or bookmaking, smuggling, theft and burglary, blackmail, loan-sharking, etc.

The term TF includes the financing of terrorist acts, terrorists and terrorist organizations. TF may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes. It is also possible that the source of funds for terrorists is perfectly legitimate or a combination of lawful and unlawful sources.

Documentation

Means digital scan copies of legal IDs, Proof of Address, Invoice, Agreements or any documentation to support Online transactions.

Source of funds

Means the location (country/city) and bank or other institution from which funds entering the account have originated.

Source of wealth

Means the economic activity which has generated the funds or other assets which the institution is handling for the customer (e.g. inherited wealth, wealth from the sale of a business, investment income, etc).

Tipping off

A person commits an offence of 'tipping off' when he/she suspects that an authorized officer is conducting an investigation related to money laundering or suspects that a Suspicious Transaction Report has been made to an authorized officer and discloses this to a third party who is likely to prejudice the investigation.

Politically exposed person

Means a natural person who is or has been entrusted with prominent public functions domestically or in a foreign country or in an international organization. "Prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executives of state owned corporations, senior political party officials, members of the legislature and senior management of international organizations.

.

APPENDIX 2 – Escalation to the AML/CFT Compliance Officer

Internal Suspicious Transaction Report to the AML/CFT Compliance Officer

STRICTLY CONFIDENTIAL

This Precedent Internal Suspicious Transaction Report (STR) form is intended for use by staff to report suspicions of money laundering, terrorist financing, bribery or corruption, property or mortgage fraud, slavery or human trafficking, tax evasion facilitation, or organised crime group involvement to the AML/CFT Compliance Officer.

Part 1: Involved parties

CUSTOMER	**Name**	*Name of customer*
	Customer Identification Number	*CIN as per Numbers if any*
	Date of birth	*Insert date of birth*
	Address	*Insert address*
	Additional details	*Insert any further details that may be known about the individual*
	Involvement	*This should indicate the involvement as you understand it of this party in the activity you are reporting*

You should create as many tables as required for your case and complete as much information as known for each party.

Part 2: Reason for suspicion

Guidance on completing this section

Provide a summary to explain your suspicion and then provide a chronological sequence of events. Try to keep the content clear, concise and simple. For example, explain how you became aware of the situation, describe the events, activities and/or transactions that led you to be suspicious, and how and why you became suspicious because of these.

"As a guide when submitting a Suspicious Transaction Report (STR), wherever you can, try to answer the following six basic questions to make the information provided as useful as possible:

- *Who?*
- *What?*
- *Where?*
- *When?*
- *Why?*
- *How?*

Remember to include:

- *the date of activity*
- *the type of product or service*
- *how the activity will, or has, taken place when documenting the reason for suspicion.*

If you are suspicious because the activity deviates from the normal activity for that individual/firm, briefly explain how the activity that gave rise to your suspicion differs from the normal."

Part 3: Supporting Documentation

Attach any supporting documentation that is relevant for the case. For example, this may include copies of correspondence, customer files or information that you have obtained on the matter. *For each file attached, ensure that an explanation is provided of what it is, as this will help when the case is being reviewed.*

Part 4: Submitter's Details

Employee name	
Contact number	
Department	
Signed	
Date of signature	

Part 5: To be completed by the AML/CFT Compliance Officer
Action taken

Observations and Decision

Signed	
Date of signature	

APPENDIX 3 – Prohibited Countries

LP will not deal with customers based in or linked to the following countries:

- Abkhazia
- Afghanistan
- Angola
- Belarus
- Burma (Myanmar)
- Burundi
- Central African Republic
- Cuba
- Democratic Republic of the Congo
- Ethiopia
- Guinea-Bissau
- Iran
- Iraq
- Ivory Coast (Cote D'Ivoire)
- Lebanon
- Liberia
- Libya
- Mali
- Nagorno-Karabakh
- Nicaragua
- North Korea
- Northern Cyprus
- Pakistan
- Palestine
- Russia
- Sahrawi Arab Democratic Republic
- Somalia
- Somaliland
- South Ossetia
- South Sudan
- Sudan
- Syria
- The Crimea region of Ukraine
- Ukraine
- Venezuela
- Yemen
- Zimbabwe