

## 1 Purpose and Policy statement

This policy details how Lion Payment UK Limited (“**the Firm**”) will manage the risks posed by money laundering and terrorist financing and ensure a consistency of approach within the firm. Please note this is a shortened version of the firm’s official policy.

The Firm is authorised by the Financial Conduct Authority (“**FCA**”) and, as such, will act in accordance with the anti-money laundering and terrorist financing rules as defined by the FCA.

The Firm has a zero tolerance for money laundering and terrorist financing and is committed to mitigating the risks of any such attempts to use the services provided by Lion Payment UK Ltd for such activity. The Firm will investigate any suspicion of money laundering and take the necessary action.

Lion Payment UK Ltd and its staff are committed to the highest standards of anti-money laundering (AML), including anti-fraud, anti- corruption and taking measures to mitigate against financial crime.

We abide by and adhere to all applicable laws and regulations regarding AML in all jurisdictions where it conducts its business. We have developed and implemented a comprehensive set of measures to identify, manage and control all AML risks.

We understand that the money laundering regulations and legislation place a responsibility upon Lion Payment UK Ltd’s employees to combat money laundering with regard to a wide area of financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime.

## 2 Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income. The risks to the financial sector primarily involve being used to facilitate this process, whether knowingly or unwittingly.

Terrorist Financing is all dealings with funds or property which are, or are likely to be, used for the purposes of terrorism, even if the funds are “clean” in origin.

### 2.1 Key stages of money laundering

Money laundering is generally broken down into in three distinct stages:

- Placement– this is the first stage in the money laundering operation and involves the physical disposal of the initial proceeds derived from illegal activity, e.g. placing cash in the conventional financial system
- Layering– this second stage involves separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity
- Integration– the final stage involves providing an apparent legitimacy to the criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

## 2.2 Money Laundering and Terrorist Financing Offences

A money laundering offence may be committed if a person:

- Conceals, disguises, or transfers criminal property
- Enters into or becomes involved in an arrangement which he knows, or suspects facilitates the acquisition, retention, use or control of criminal property on behalf of another person
- Acquires, uses, or has possession of criminal property

In the case of terrorism financing, an offence is committed if there is involvement in providing money, or other property, to be used for the purposes of terrorism, even if the funds are clean in origin.

## 3 Risk management and Controls

### 3.1 Client Due Diligence

The Firm's client due diligence consists of the following:

- Identifying the client and verifying the client's identity using documents or information from a reliable and independent source
- Identifying the beneficial owner(s) and verifying that person's identity, taking measures to understand the ownership and control structure of the client, where applicable
- Assessing the purpose and intended nature of the business relationship (business profile)
- Conducting ongoing monitoring of the business relationship and transactions undertaken to ensure that they are consistent with the Firm's knowledge of the client, business, risk profile and source of funds

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

The Firm will ensure that clients are identified and that their identity is verified before commencing any transactions with them.

#### 3.1.1 Corporate clients

##### 3.1.1.1 Identifying corporate clients

The Firm will obtain the following information for prospective clients that are corporates:

The Firm's current policy is NOT to onboard clients under this classification.

- Full name
- Registered number
- Registered office in country of incorporation
- Business address

And for private or unlisted companies:

- Names of all the directors
- Names of individuals who own or control over 25% of its shares or voting rights

- Names of any individuals who exercise control over the management of the company
- Names of ALL beneficial owners (where practicable) for Sanctions and PEP screening
- The Firm will take reasonable steps to identify the beneficial ownership and controllers of the corporate. It will keep records of the actions taken to determine such.

#### **3.1.1.2 Verifying identities of corporate clients**

The Firm will verify the identity of the client by confirming the company's listing on a regulated market, searching the relevant company registry or viewing a copy of the company's Certificate of Incorporation. If there is a discrepancy between the company register and the client information, then the Firm will update the company register with the correct information.

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

### **3.1.2 Unincorporated clients**

#### **3.1.2.1 Identifying unincorporated clients**

The Firm will obtain the following information for prospective clients that are unincorporated:

- Full name
- Business address
- Names of all the partners/principals who exercise control over the management of the business
- Names of individuals who own or control over 25% of its capital/profit or voting rights

#### **3.1.2.2 Verifying identities of unincorporated clients**

The Firm will verify the identity of the client by using information from an independent and reliable source, confirming the client's membership of a relevant professional or trade association, viewing the partnership deed or treating the client as a collection of private individuals.

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so.

### **3.1.3 Public sector body, government, state owned company and supranational clients**

#### **3.1.3.1 Identifying public sector body, government, state owned company and supranational clients**

The Firm will obtain the following information for prospective clients that are public sector bodies, governments, state owned companies or supra-nationals:

- Full name of entity
- Nature and status of entity
- Address of the entity
- Name of the home state authority
- Names of directors

### **3.1.3.2 Verifying identities of public sector body, government, state owned company and supranational clients**

The Firm will ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

#### 3.1.4 Pension scheme clients

The Firm will check the

#### 3.1.5 Nature of Business

The Firm will obtain and record sufficient information on the client's nature of business and the purpose of the account, including expected source of funds, source of wealth and anticipated transaction volumes and values. This will enable an assessment of whether the purpose of the account to be opened is consistent with the nature of business.

## 3.2 Customer Risk Assessment

The Firm will assess the risk for each client considering the purpose of the account or relationship, the level of assets involved or the size of transactions to be undertaken and the regularity or duration of the business relationship.

The client risk assessment will also consider customer risk factors (including nature of business), product, service, transaction or delivery channel risk factors and geographical risk factors.

## 3.3 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is performed by The Firm when clients are identified with any high-risk factors for financial crime, however the extent of the enhanced due diligence will depend on the reason why a relationship with the client is classed as high risk. The Firm will take an informed decision, agreed with the Nominated Officer, about which enhanced due diligence measures are appropriate in each high-risk situation.

## 3.4 Financial Sanctions

The Firm will review all clients to ensure that they are not on the Financial Sanctions register as published by HM Treasury or other relevant body (e.g.OFAC), at initial client set up and then periodically on a risk based approach. The Firm will not set up accounts for clients on the Financial Sanctions Register or carry out any transactions with them. The Firm will screen all incoming and outgoing transaction beneficiaries for Sanctioned status.

It is a criminal offence to make funds or financial services available to individuals or entities on the sanctions list without a licence. The latest list can be found here:

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

The Firm will complete checks on clients to ensure that they are not on the financial sanctions register before proceeding with the account set up.

Employees will discuss any clients that appear on the sanctions list with the MLRO in the first instance. If a prospective client is on the sanctions list and the Firm does not hold a relevant licence to proceed, then the

Firm will halt further account set up and report the matter to the Office of Financial Sanctions at the HM Treasury – contact details as follows:

Office of Financial Sanctions Implementation  
HM Treasury  
1 Horse Guards Road  
London SW1A 2HQ

TEL. 020 7270 5454 or email [ofsi@hmtreasury.gsi.gov.uk](mailto:ofsi@hmtreasury.gsi.gov.uk)

The Firm has subscribed to email updates of the sanctions list on the HM Treasury website (<https://public.govdelivery.com/accounts/UKHMTREAS/subscriber/new>) to keep up to date with any changes. New additions to the list will be checked against the Firm's existing client lists and any positive matches will be reported to the Office of Financial Sanctions at the HM Treasury immediately and any funds or transactions will be frozen.

The Firm will continually monitor the client lists against the sanctions list and any positive matches will be reported to the Office of Financial Sanctions at the HM Treasury immediately.

## 4.1 Ongoing Monitoring

The Firm will continually monitor its clients for signs of money laundering, focusing on transaction monitoring and client reviews.

### Red Flags

Red flags are client behaviours or issues with client's business that should act as a warning that further investigation by the Firm is necessary.

### Transaction monitoring

The Firm will continuously monitor client's transactions to detect unusual transactions or patterns of transactions and to ensure that any unusual or suspicious activity is identified and investigated immediately.

### Client reviews

The Firm will ensure that client due diligence information is relevant and kept up to date via regular client reviews. The extent to which client reviews are undertaken will be determined using a risk-based approach and applied in accordance with the risk rating applied to the client during the client risk assessment.

The Firm has a customer review process based on the High, Medium, and Low risk factors assigned to its customers

#### 4.1.1 Trigger events

In addition to the scheduled reviews above, if the Firm, through the course of its daily activities, obtains information that brings question to the accuracy of the client due diligence information collected, or if a suspicion arises, then the client will be undergo an immediate review, irrespective of their risk status.

## 5.1. Reporting Suspicious Transactions

Employees are expected to be alert to money laundering terrorist financing attempts and they are responsible for reporting any actual or suspected money laundering and / or terrorist financing attempts to the MLRO in a timely manner.

If suspicious signals of money laundering and / or terrorist financing are identified, the transaction should be frozen and should not proceed without the authorisation of the Nominated Officer. All suspicious signals of money laundering and / or terrorist financing are reportable, even if it comes to the employees' attention after the trade has been undertaken or the account is closed, or the trade has been conducted by another person.

Where there is serious suspicion, evidence, or reasonable grounds for suspecting, that a transaction may be deemed suspicious, employees are required to report their suspicions in accordance with the Firm's procedures on Suspicious Transaction Reporting.

The MLRO will receive any reports or concerns relating to any suspected or actual money laundering and will record, investigate, and report this to the relevant authorities, such as the National Crime Agency ("**NCA**"), where necessary. If reports are not forwarded to the relevant authorities, full details of the rationale for this decision will be kept on record.

All notifications made will be handled with strict confidentiality. However, please note that there may be circumstances in which The Firm is required to reveal an individual's identity, for example where we are compelled to do so by law and therefore anonymity cannot be guaranteed.

If there are concerns about any repercussions of making a suspicious transaction report, then the Whistleblowing Policy and Procedure should be followed for information on alternative methods of making a report.

Failure to notify an appropriate person about criminal actions of which an employee is or should have been aware, in breach of this policy, may be considered a contractual breach leading to disciplinary actions or personal criminal liability.

All staff will receive training at least annually (and more frequently if regulation changes arise) and will be asked to attest their adherence to the internal procedures. A record of all training will be kept on the training log.

### 5.1.1 Subsequent investigations

The Firm is committed to supporting regulators and law enforcement officers in the prevention of financial crime.

All employees are expected to cooperate fully with any investigations. Employees must also recognise, however, that laws and procedures may apply to the disclosure of information and they should therefore contact the MLRO before disclosing information about clients or employees when contacted directly by law enforcement officers.

Refer to JMLSG Guidance – *Prevention of money laundering/combating terrorist financing Part II Sectoral Guidance* for sector specific guidance.

