LYNKPAY LTD.

Anti-Money Laundering Policy

Version 1.0 (2022)

ANTI MONEY LAUNDERING POLICY (AML)

1. INTRODUCTION AND PURPOSE

1.1 Money laundering is the process of introducing money, property or other assets derived from illegal and criminal activities into the legal financial and business cycle to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin.

1.2 The definition of money laundering has been increased and the range of activities caught by the money laundering framework has been wider. It is no longer merely an issue for banks and the financial sector but now applies to all companies and institutions. These new obligations require companies to establish internal procedures to prevent the use of their services for money laundering.

1.3 The purpose of this AML Policy is to provide guidance to Lynkpay Ltd. employees on how to strengthen anti-money laundering governance and reiterates the Company's commitment to full compliance to the Money Laundering regulations.

2 SCOPE

2.1 This Policy establishes the general framework for Lynkpay Ltd. to manage and prevent the risks of Company's businesses from being used as a conduit for money laundering and terrorism financing activities. All employees are required to adhere to the requirements of this Policy when carrying out their daily responsibilities.

2.2 This Policy sets out the procedures that must be followed to enable Lynkpay Ltd. to comply with its legal obligations. Lynkpay Ltd. employees who need to be the most vigilant are those dealing with the receipt or outlay of funds whether in the form of cash, cheques or bank transfer.

3 DEFINITIONS

3.1 Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty' funds and converts them into other assets so they can be reintroduced into legal commerce. This process conceals the true origin or ownership of the funds and so 'cleans' them. The legislation defines the offences relating to money laundering as:

- Concealing, disguising, converting or removing criminal property;
- Entering into an arrangement which the person who knows or suspects or facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;

- Acquiring, using or having possession of criminal property;
- Making a disclosure which is likely to prejudice a money laundering investigation

4 GENERAL DESCRIPTION OF MONEY LAUNDERING

4.1 Money laundering regulations generally applies to cash transactions in excess of 10,000 Pound Sterling. However, it now applies to all transactions – cheques, cash, bank transfers, property and equipment to individuals or agents or third parties.

4.2 The Company will adopt a risk-based approach to anti-money laundering and in how they conduct due diligence.

- **Risk assessment:** Lynkpay Ltd. will appoint Money Laundering Reporting Officer (MLRO) to analyses potential exposure to money laundering or terrorist financing. A written AML risk report should cover all activities including customers, countries of operation and services, transactions, delivery channels and size and nature of business.

- **Risk mitigation:** Policies will be in writing of how we mitigate risk, proportionate to the risks identified, approved annually by senior management. To include relevant controls, customer due diligence procedures, reporting, record keeping and monitoring.

- **Level of Customer Due Diligence (CDD):** To undertake CDD appropriate to the risk with specific attention on high-risk jurisdictions which make enhanced due diligence compulsory.

- **Politically Exposed Persons (PEPs)**: To undertake due diligence of individuals who are trusted with prominent functions.

4.3 As part of the risk-based approach, Lynkpay Ltd. will periodically and at least annually update the risk assessment and review the policies and procedures to ensure they take account of the changing risks and vulnerabilities of Lynkpay Ltd. Assessment of risk will be made by the Money Laundering Reporting Officer (MLRO) in conjunction with appropriate line management.

5 RISKS WHICH THE COMPANY MAY BE EXPOSED

5.1 While Lynkpay Ltd. financial activity could be considered relatively medium to high risk from the perspective of money laundering, all staff need to be vigilant against the financial crime and fraud risks of the day-to-day transactions. Any suspicious transaction shall be reported promptly to the MLRO. To counter the risk of Company becoming accidentally involved in money laundering, the principal risks need to be identified, assessed and procedures shall be put into place to mitigate the risks.

5.2 Various Anti-Money Laundering reports suggests that particular care should be focused on:

- Any payments in cash
- Unidentified cash receipts
- Applicants from high-risk countries
- Requests for refunds – (particularly to a different account or individual to the payer)
- Overpayments
- Identity fraud

5.3 Typically, these would include:

- Product/Service and Distribution Cash transactions, anonymous transactions, non-face-to face transactions, transactions involving unknown third parties and unregulated transactions (i.e. from unregulated third-parties)

- Customer/Third-Party Unusual business relationships, cash businesses, non-local residents and Politically Exposed Persons (PEP's) and Sanctioned Parties.

- Country, geographic and jurisdictional Countries recognised to have inadequate AML/CTF controls and processes, countries subject to sanctions, embargoes and related measures and Composite Risk countries identified by recognised authorities as supporting terrorism and/or terrorist organisations.

5.4 With regard to customers, and, where applicable, their beneficial owners (BOs):

- Their business or professional activity;
- Their reputation; and
- Their nature and behavior, including whether their behavior could point to heightened ML/TF risks;
- Their links to sectors commonly associated with higher corruption risks;
- Their links to sectors commonly associated with higher ML/TF risks;
- Their links to sectors the operations of which involve significant amounts of cash;
- For customers who are legal persons, trusts or other legal arrangements, theirpurpose and the nature of their business;
- Their links to, or classification as Politically Exposed Persons (PEPs);
- Their prominence, public profile, influence and decision-making power;
- The enforceability of identity and beneficial ownership disclosure requirements(e.g. mandatory for publicly traded companies);
- Their effectiveness of the customer's local AML/CTF regime and the country's riskprofile in terms of corruption levels;
- Their inclusion into sanctions lists; and

- The consistency of business information and plans provided by the customer withrespect to the information previously received by the firm;
- Existence of adverse media reports;
- Current or past investigations for terrorist activity or personal or professional links to persons under such investigations;
- Current or past administrative or criminal proceedings;
- Seizing or freezing of assets;
- Previous suspicious activity or transaction reports; and
- Previous business relationship.

5.5 With regard to countries and geographical areas:

- The jurisdiction where the customer and/or the BO are residents;
- The jurisdiction which are the main places of business for the customer and/or the BO;
- The jurisdictions to which the customer and/or the BO have relevant personal or business links, including legal and financial interests;
- The level of predicate offenses to ML and the effectiveness of a country's legal system;
- Information about known groups committing terrorist offences in a jurisdiction;
- The extent to which the operation of groups committing terrorist offences in a jurisdiction could be expected to give rise to suspicion about the nature and purpose of a business relationship;
- The adequacy of a country's AML/CTF regime and supervision;
- Information about a jurisdiction providing funding or support for terrorist activities, whether from official sources, or from groups or organizations in such jurisdiction;
- The jurisdiction being a subject of financial sanctions, embargoes or other measures related to terrorism, financing of terrorism or proliferation;
- The adherence and compliance of a jurisdiction to FATF 40 Recommendations, tax transparency and information sharing standards, Common Reporting Standard orAutomatic Exchange of Information; and
- Existence of reliable and accessible beneficial ownership registers.

5.6 With regard to products, services and transactions:

- The level of transparency (or opaqueness) these afford;
- The capacity of customers or BOs to remain anonymous or hide their identity;
- The influence of third parties not part of the business relationship over the

business relationship

- Their complexity;
- Their involving of multiple parties and/or jurisdictions;
- Their regularity;
- Their acceptance of payments from third parties, or overpayments where theseare not to be expected;
- Their value or size;
- Their sensitivity to cash;
- Their capacity to facilitate or encourage high-value transactions.

5.7 With regard to delivery channels:

- The extent to which the business relationship is conducted on a non-face-to-facebasis;
- The physical presence of a customer for identification purposes;
- The usage of a reliable form of non-face-to-face CDD tools and procedures;
- The steps taken to prevent impersonation or identity fraud;
- The nature of the relationship between any intermediaries used by the firm and the firm itself;
- The reliability of an introduction of a customer by another part of the same financial group, if such an introduction takes place;
- The reliability of the third party executing the introduction, including whether they are subject to AML obligations, whether they apply CDD measures consistent with the standards imposed, and whether they are based in a jurisdiction associated with higher ML/TF risks;
- Where agents are used, the level to which agents have obtained sufficient information collected by the agent about a customer;
- Where outsourcing is used, the considerations given about the outsourcing service provider being compliant with its AML/CTF.

5.5 Lynkpay Ltd.'s Anti-Money Laundering risk assessment covers all areas and assesses each of the above risk factors and rates them on a RAG (Red, Amber, Green) scale equating to High, Medium and Low.

6 POLICY STATEMENT

6.1 Lynkpay Ltd. strongly objects to all practices related to money laundering, including dealing inthe proceeds of criminal activities and terrorism financing. As a general rule, reasonable degree of due diligence must be carried out in order to understand the business and background of any prospective customer, vendor, third party or business partner that intends to do business with Lynkpay Ltd. to determine the origin and destination of money or assets involved. Any suspected

activities relating to money laundering or terrorism financing should be reported immediately to relevant authorities.

6.2 Lynkpay Ltd. prohibits all involvement in money laundering activities and terrorism financing either directly or indirectly. The activities may include, but not limited to the following:

- Payments made in currencies that differ from invoices;
- Attempts to make payment in cash or cash equivalent (out of normal business practice);
- Payments made by third parties that are not parties to the contract; and
- Payments to or from accounts of third parties that are not parties to the contract.

7 CONTROLS TO MITIGATE RISK

7.1 Lynkpay Ltd. will pursue a policy of maximising online payments. All payments should be made through online payment systems thereby removing acceptance of cash.

7.2 Payments by third party:

- Where identified, details to be checked over £5,000.
- Refunds of payments will only be made by the same method and to the same account as the original payment was made.
- There will be no cash refunds.

8 CUSTOMER DUE DILIGENCE

8.1 As a general principle, all employees are required to perform customer due diligence (CDD) procedures when:

a) at the start of a new business relationship;
b) it has any suspicion of money laundering or terrorism financing activities regardlessof the amount transacted;
c) it has any doubt about the adequacy or authenticity of previously obtained information.

8.2 Lynkpay Ltd. must be reasonably satisfied as to the identity of the customer to discharge the ‘reasonably satisfied’ requirement. Lynkpay Ltd. must, for example, know the name, permanent address and/or date of birth, as part of the CDD processes before commencing a business relationship.

8.3 There are three levels of CDD - ‘Standard’, ‘Simplified’, and ‘Enhanced’. ‘Standard due diligence’, as outlined above, should be applied to all financial relationships unless ‘simplified’ due diligence is or ‘enhanced’ due diligence is appropriate.

8.4 The CDD procedures should minimally include:-

a) identifying the customer (including foreign body corporate) and verify such customer's identity using reliable, independent source of documents, data or information;

b) verifying that any person purporting to act on behalf of the customer is authorised, and identifying and verifying the identity of that person;

c) identifying and take reasonable measures to verify the identity of the beneficial owner(s), using relevant information or data obtained from reliable sources;

d) understand and, where relevant, obtain information on the purpose of opening an account and the intended nature of the business relationship; and

e) where necessary, performing appropriate background checks, where practical and relevant, on the names of individuals or entities of customers to ensure that transactions are not entered with those listed on the sanction lists maintained by United Nations Security Council.

9 SUSPICIOUS TRANSACTION REPORTING

9.1 If any suspicious money laundering or financing of terrorism activities are detected or anyattempted transaction fits the list of "Red Flags" as in the table below, these transactions must be reported to Money Laundering Reporting Officer (MRLO) immediately via an Internal Suspicion Report:-

Examples of "Red Flags" – Possible Suspicious Transactions
• Reluctance to provide detailed information of the source of income. • Large cash transaction with no history of prior business experience. • Shielding the identity of the beneficial owners. • Requests for account details outside the normal course of business. • Cancellation, reversal or request for refunds of earlier transactions. • Transferring of funds from third party or foreign bank accounts. • Requests for payments or refunds after funds have been paid into Company's bank account by a third party • Payment of any substantial sum in cash • A secretive person or business e.g. that refuses to provide requested information without a reasonable explanation

9.2 Upon receiving the Internal Suspicious Transaction Report, the MRLO shall evaluate the grounds and if confirmed he or she shall submit a suspicious

transaction report to the relevant authorities on the next working day.

10 DUTIES OF MONEY LAUNDERING REPORTING OFFICER

10.1 The MLRO will consider the notification and any other available internal information considered relevant, such as:

- Reviewing other transaction patterns and volumes.
- The length of any business relationship involved.
- The number of any one-off transactions and linked one-off transactions.
- Any identification evidence held and undertake such other reasonable enquiries he/she thinks appropriate in order to ensure that all available information is considered in deciding whether a report to authorities is required

10.2 The MLRO may also need to discuss their report with the employee. The MLRO should keep a copy of all reported suspicious transactions together with additional backup and reasons for final conclusions, whether reported to the authorities or not for a minimum of 2 years.

11 TRAINING & COMMUNICATIONS

11.1 In line with the Regulations, all relevant members of staff shall receive training in this policy and the wider aspects of AML. This will include new members, where the training will first be completed as part of their induction.

11.2 Record keeping is crucial to an effective training regime and a signed record (or computer-based equivalent) from every member of staff should be kept verifying that they have read, understood, and been trained on AML and the policy.

11.3 The frequency of training for relevant staff should be determined on a risk-based approach but the periodicity should not exceed two years, with annual training being used where it is warranted by the potential risk. In addition, refresher training should take place at each revision of the policy.

12 RECORDS KEEPING AND RETENTION OF RECORDS

12.1 Lynkpay Ltd. must keep record of all transactions and ensure they are up to date and relevant. The records must at least include the following information for each transaction:

a) Documents relating to the identification of the customer in whose name the transaction is executed.

b) The identification of the beneficial owner or the person on whose behalf thetransaction is executed.
c) Records of the relevant account pertaining to the transaction executed.
d) The type and details of transaction involved.
e) The origin and the destination of the funds, where applicable; and
f) Any other information as required by the authorities.

12.2 Lynkpay Ltd. employees are required to retain, for at least five (5) years, the records of transactions, relevant customer due diligence information and other relevant records including agreements, financial accounts, business correspondences and documents relating to the transactions in a form that is admissible as evidence in court and make such documents available to authorities and law enforcement agencies in a timely manner.

13 RESPONSIBILITY FOR THE POLICY

13.1 This Policy is reviewed and approved by the Board and the oversight of this Policy has been delegated to the Lynkpay Ltd. Management team, which monitors the effectiveness and compliance of this Policy.

13.2 Lynkpay Ltd. Management team set the tone at the top providing leadership and support for the Policy and take responsibility for its effectiveness within their business units. Lynkpay Ltd. Management is responsible for the implementation of the Policy and all communication and training activities in relation to the Policy to ensure that those reporting to them are made aware of, and understand, this Policy.

13.3 Prompt action is expected of all employees, referring to the guidance in this policy. Any suspicions employees are asked to consult their line manager or MLRO about the concerns.

14 EFFECTIVE DATE

14.1 The Policy is approved by the Company and effective as of 17th of December, 2022.