# Lotus Mao Payments Ltd.
# AML/CTF Compliance Program

JANUARY

2025

The Policy applies to all Lotus Mao Payments Ltd. employees, all units in the Lotus Mao Payments Ltd., senior management, foreign correspondents, contractors and third parties with whom Lotus Mao Payments Ltd. may contract with.

The aim of the Lotus Mao Payments Ltd. is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the Lotus Mao Payments Ltd. of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity.

The Policy is updated at least once a year, or more frequently based on international requirements and legislative changes, particularly with the implementation of the Canadian Payments Act, Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) or Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTF Regulations) and associated Regulations or Financial Transactions and Reports Analysis Centre (FINTRAC) Guidance on the Risk-Based Approach and Compliance program requirements.

Introduced and approved by: Arvis Valka

# Glossary

| Terms/Acronyms | Definition |
|---|---|
| MSB | Money Service Business |
| Nominated Officer | A Nominated Officer (also known as the MLR officer or AML Compliance Officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues. |
| Supporting Officer | A person or persons nominated to act on behalf of the Nominated Officer. |
| AML | Anti-Money Laundering |
| CTF | Counter-Terrorism Financing |
| KYB | Know Your Business |
| KYC | Know Your Customer |
| CDD | Customer Due Diligence |
| EDD | Enhanced Due Diligence |
| PCMLTFA | Proceeds of Crime (Money Laundering) and Terrorist Financing Act |
| FINTRAC | Financial Transactions and Reports Analysis Centre |
| PEP | Politically Exposed Persons |
| STR | Suspicious Transaction Report |
| RCMP | Royal Canadian Mounted Police |
| CSIS | Canadian Security Intelligence Service |
| SWIFT | Society for Worldwide Interbank Financial Telecommunications |
| OFAC | Office of Foreign Assets Control |
| OFSI | Office of Financial Sanctions Implementation |
| FATF | Financial Action Task Force |
| FinCEN | The Financial Crimes Enforcement Network |
| UBO | Ultimate Beneficial Owner |
| EU | The European Union |
| UN | The United Nations |
| RPAA | Retail Payment Activities Act |
| RPAR | Retail Payment Activities Regulations |
| Company | Lotus Mao Payments Ltd.<br>Registration Certificate BC1406445<br>License M23180646 on 17.08.2023 by Financial Transactions and Reports Analysis Centre of Canada<br>Address: MEZASTEPES - 6 KALSNAVAS PARISH, MADONAS NOVADS, LATVIA LV-4860 |

| | |
|---|---|
| RCS | Risk Control System (RCS), that covers 24/7 Sanction, PEP Screening as well as prevention of fraud scenarios and detection of suspicious transactions, identification of operational risks, control of breakdowns, responding to and recovering from incidents; review, testing and improvement of Risk Management Framework. RCS collects and analyzes such data as IP address, operation type, Customer ID etc. |

# Table of contents

# Introduction

Lotus Mao Payments Ltd. has developed a AML/CTF Compliance Program that meets legislative requirements and reflects principles on managing money laundering and terrorist financing risks posed to the company.

Lotus Mao Payments Ltd. is registered with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") as a Money Service Business ("MSB") and cooperates fully with FINTRAC and other law enforcement agency requests in their efforts to detect, prevent, and deter money laundering and terrorist financing. Lotus Mao Payments Ltd. is registered as a Payment Service Provider (PSP) with the Bank of Canada and is subject to the regulatory regime of Retail Payment Activities Act (RPAA) and regulations thereunder (PRAR).

**Prevention of money laundering & terrorist financing in Canada**

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

It also covers money, however acquired, which is used to fund terrorism. Terrorist financing 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.

There are three common stages in the laundering of money, and they frequently involve numerous transactions.

An MSB should be alert to any such sign for potential criminal activities. These stages are:

- Placement which involves placing the proceeds of crime in the financial system.
- Layering which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
- Integration with placing the laundered proceeds back in the economy to create the perception of legitimacy.

In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

Terrorist financing relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism or with the intention to dispose those funds to a terrorist group or a separate terrorist.
Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Criminal property is the proceeds of criminal conduct. This includes any type of conduct, wherever it takes place, which would constitute a criminal offence if committed in Lotus Mao Payments Ltd. It includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion. It also includes any other offence that is committed for profit.

Lotus Mao Payments Ltd. has established its AML/CTF Compliance Program to ensure that any money laundering risks identified by Lotus Mao Payments Ltd. are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the company being used to facilitate any financial crimes.

This program is designed to represent the basic standards of Anti-Money Laundering and Combating Terrorism Financing procedures and standards, which will be strictly observed by Lotus Mao Payments Ltd.
The AML/CTF Compliance Program is based upon applicable AML/CTF laws, regulations and regulatory guidance from the Government of Canada. This program is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation. It also follows the AML principles of the Wolfsberg Group.

# AML/ CTF systems

## 1. The primary legislation governing AML / CTF in Canada

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) The PCMLTF Regulations set out specific requirements, including:

- the appointment of a person responsible for the compliance program;
- the development and application of compliance policies and procedures that are up to date and approved by a senior officer;
- a program to assess the risk of a money laundering or terrorist financing offence being conducted through the firm, and implementation of measures to mitigate high-risk scenarios;
- an ongoing written compliance training program for employees of the Lotus Mao Payments Ltd.;
- a review of policies and procedures to test their effectiveness to be conducted every two years by an internal or external auditor.

PCMLTFA and latest redaction of FATF recommendations set out the requirement for relevant businesses to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

- Customer due diligence
- Reporting
- Record keeping
- Internal control
- Risk assessment and management (Risk Based Approach)
- The monitoring and management of compliance, and
- The internal communication of such policies and procedures, in order to prevent activities related to money laundering and terrorist financing and proliferation financing. These policies and procedures must:
- Identify and scrutinize
- Complex or unusually large transactions

- Unusual patterns of transactions which have no apparent economic or visible lawful purpose
- Any other activity which could be considered to be related to money laundering or terrorist financing or proliferation financing
- Specify the additional measures that will be taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing
- Determine whether a customer is a politically exposed person
- Nominate an individual in the organization to comply with, and receive disclosures under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.
- Ensure employees report suspicious activity to the Nominated Officer, and
- Ensure the Nominated Officer considers such internal reports in the light of available information and determines whether they give rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

The main principles encompassed by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations can be described as Risk Based Approach (RBA). RBA requires several steps to be taken to determine the most cost-effective and proportionate way to manage and mitigate the money laundering and terrorist financing and proliferation financing and sanctions violation risks faced by the business. The steps are to:

- Identify the money laundering and terrorist financing and proliferation financing and sanctions violation risks that are relevant to the business
- Assess the risks presented by the particular:
  - Customers – types and behavior;
  - Products and services
  - Geographical areas of operation, for example, location of business premises, source or destination of customers' funds;
  - Complexity and volume of transactions;

- Design and implement controls to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls and
- Record appropriately what has been done, and why

## 2. Effective controls

To ensure proper implementation of AML/CTF procedures and controls, Lotus Mao Payments Ltd. has effective controls covering:

- Effective AML/CTF compliance program
- Senior management oversight
- Appointment of Compliance Officer / Money Laundering Reporting Officer (MLRO)
- Compliance and audit function
- Staff screening and training.

Lotus Mao Payments Ltd. firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The company is, therefore, committed to the highest standards of Money Laundering and Combating Terrorism financing (AML/CTF) measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

## 3. The Money Laundering Reporting Officer (Nominated Officer)

A Nominated Officer is the person within an organization who is responsible for overseeing all activity related to anti-money laundering matters.

Lotus Mao Payments Ltd's Nominated Officers should remain up-to-date with AML/ATF rules and risks.

The Nominated Officer's responsibilities include:

- Receiving disclosures from employees (also known as Suspicious Transaction Report - STR's).
- Deciding if disclosures should be passed on to the Financial Transactions and Reports Analysis Centre or the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS).
- Reviewing all new laws and deciding how they impact on the operational process of thecompany
- Preparing a written procedures manual and making it available to all staff and other stakeholders
- Making sure appropriate due diligence is carried out on customers and business partners
- Receiving internal Suspicious Transaction Report (STR) from staff
- Deciding which internal STR's need to be reported on to FINTRAC or RCMP or CSIS.
- Recording all decisions relating to STRs appropriately
- Ensuring staff receive anti-financial crime training when they join and that they receive regular refresher training
- Monitoring business relationships and recording reviews and decisions taken
- Making decisions about continuing or terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction as per FINTRAC regulations.

The Nominated officer is a person who has sufficient authority and autonomy in order to make the decisions required above. The Supporting Nominated Officer shall replace the Nominated Officer when he/she is unavailable.

## 4. Staff Training

Lotus Mao Payments Ltd. maintains an on-going employee training program so that the staff is adequately trained in KYC procedures and that the staff is aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers/Merchants. New staff is educated in the importance of KYC policies and the basic requirements at the Company.

Training is given to all staff members upon commencement of taking on the position in the Lotus Mao Payments Ltd. and on regular occasions afterwards (at least once a year). Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities or sanctions violation typologies.

Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Training covers the following issues:

- The law relating to financial crime;
- Risks associated with the financial crime threat to the company (see, for example, www.egmontgroup.org);
- Identity and responsibilities of the Nominated Officer;
- Internal policies and procedures put in place;
- Customer Due Diligence/Enhanced due diligence monitoring measures;
- Suspicious activity – what to look out for;
- How to submit an internal Suspicious Transaction Report to the Nominated Officer;
- Record-keeping requirements;
- Possible sanctions violation – what to look out for;

The Nominated Officer will keep a log of all training which is provided to staff members. All staff will be required to sign the training log where required to confirm that they have received training.

The Nominated Officer will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all company's locations.

The Nominated Officer shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report. Lotus Mao Payments Ltd. will use the Canadian Anti-Money Laundering Institute training programs and offered training sessions for regular updates of internal training programs (https://www.camli.org ). Also Lotus Mao Payments Ltd. will use others learning possibilities which are offered by well-known and reputable organizations (for example ACCP, ACAMS, ICA).

# Risk-based approach (RBA)

## 1. Risk assessment and risk categories

The object of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its Regulations is to detect and deter money laundering and terrorism financing. In 2008, the Government introduced amendments to the PCMLTFA and its Regulations to enhance the Canadian anti-money laundering and anti-terrorism financing (AML/ATF) regime. As part of these amendments, the Risk-Based Approach (RBA), which requires reporting entities to conduct assessments of their exposure to money laundering and terrorism financing risk using a number of prescribed criteria, was introduced.
Risk may be established both on the basis of objective criteria and subjective criteria. A 'risk rating' is given to each criterion.

The Company, as part of its AML Program, has conducted a risk analysis to identify specific criteria of potential money laundering risks. This risk based approach includes the identification of the money laundering and terrorist financing risks (to the extent that such terrorist financing risk can be identified) of customers, categories of customers, and transactions that allow the Company to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment is routinely performed at the inception of a customer relationship, for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account. Thus, the monitoring of customer transactions and ongoing reviews is a fundamental component of the Company's risk based approach. In addition, this type of risk assessment process may also be adjusted for a particular customer based upon information received from a competent authority.
The Company measures money laundering and terrorist financing risks using the following categories. The application of risk categories provides a strategy for managing potential risks by enabling the Company to subject customers to proportionate controls and oversight. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary depending on the Company's unique circumstances.

**Low Risk** – entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk, Government Departments and Government owned companies, regulators and statutory bodies etc. Generally clients with a small number or transfers and small dollar transactions would be considered LOW RISK.

**Medium Risk** – customers that are likely to pose a higher than average risk to Lotus Mao Payments Ltd. may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds.

**High Risk** – Lotus Mao Payments Ltd. applies enhanced due diligence measures based on the risk assessment for higher risk customers, especially those for whom the sources of funds are not clear.

To all customers classified as high risk the procedure of enhanced due diligence is applied. The main criteria to rank the client as high risk are the following:

- the high risk jurisdiction domiciles of customers;
- the high risk or prohibited industries or activities of customers;
- complex shareholder structure with hidden UBOs;
- UBOs, PEPs, US-citizens as shareholders or key management personnel;
- restrictions or sanctions imposed on customers by regulatory authorities;
- nonresident customers;
- Politically Exposed Persons (PEPs) accounts;
- customers from countries that are considered by the FATF inadequately to apply the FATF Recommendations;
- transactions that are unusual, lack an obvious economic or lawful purpose;
- transactions that are complex or large or might lend themselves to anonymity;
- trusts, charities, NGOs and organization receiving donations;
- any other customers that their nature entail a higher risk of money laundering or terrorist financing;
- customers with dubious reputation as per public information available.

Lotus Mao Payments Ltd. categorizes the following categories of customers as high-risk customers:

- High Net worth individuals in the company's shareholder structure
- Trusts, charities, NGOs and organizations receiving donations
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'
- Politically Exposed Persons (PEPs) of foreign origin
- Companies issuing bearer shares
- Trade of oil products
- Trade of new financial products (e.g. virtual currencies)
- Those with dubious reputation as per public information available
- Organization and execution of auctions

**Country or Geographic Risk**

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Factors that may result in a determination that a country poses a higher risk include: Countries subject to sanctions, embargoes or similar measures issued by the United Nations ("UN") as an example. In addition, some circumstances subject countries to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by the Company because of the standing of the issuer and the nature of the measures;

Countries identified by credible sources as lacking appropriate AML laws, regulations and other measures. The term "credible sources" refers to information that is produced by well known bodies that are generally regarded as reputable and that make such information publicly and widely available.

In addition to Canadian Financial Action Organizations' other sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organizations. The

information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk; Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them; or Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

The risk associated with countries and geographical areas, Lotus Mao Payments Ltd. consider the risk related to:

- the jurisdictions in which the customer and beneficial owner are based;
- the jurisdictions that are the customer's and beneficial owner's main places of business; and
- the jurisdictions to which the customer and beneficial owner have relevant personal links.

The company defines a list of jurisdictions with which it does not cooperate, as well as a list of high-risk countries based on FATF high-risk and other monitored jurisdictions, The Basel AML Index, Transparency International index, Canadian and U.S. sanctions programs etc.

Lotus Mao Payments Ltd. does not handle transactions or onboard any customer fromnon-cooperation countries list.

**Customer Risk**

Determining the potential money laundering or terrorist financing risks (to the extent that such terrorist financing risk can be identified) posed by a customer or category of customers is a critical component. Based on its own criteria, the Company is able to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. The application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include: Customers conducting their business relationship or transactions in unusual circumstances, such as:

- Significant and unexplained geographic distance between the Company and the location of the customer;
- Frequent and unexplained movement of accounts to different institutions; and
- Frequent and unexplained movement of funds between institutions in various geographic locations.

The structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests of the customer.

**Product and Service Risk**

This category of risk includes the determination of potential risks presented products and services offered by the Company, such as risks associated with new or innovative products or services and the following factors:

- Services identified by competent authorities or other credible sources as being potentially higher risk;
- Services involving banknote and precious metal trading and delivery; or
- Services that inherently have provided more anonymity or can readily cross international borders, such as online banking, stored value cards, private investment companies and trusts.

**Third-party services**

If company receives services related to a payment function from one or more third-party service providers, the risk management and incident response framework must:

- address the means by which the payment service provider will — no less than once a year in respect of each of its third-party service providers and before entering into, renewing, extending or substantially amending a contract with a third-party service provider for the provision of a service related to a payment function — assess
- the third-party service provider's ability to protect data and information that they obtain from the payment service provider or in the course of performing services for it,
- the security of the third-party service provider's connections to and from the payment service provider's systems,
- the manner in which the third-party service provider's performance may be monitored, including the time and manner in which the third-party service provider will inform the payment service provider of any detected breach of the payment service provider's or the third-party service provider's data, information or systems and of any other deterioration, reduction or breakdown in the services provided to the payment service provider, and

the third-party service provider's risk management practices in relation to the services that they provide to the payment service provider;
clearly allocate responsibilities between the payment service provider and the third-party service.

**Other Risk Variables**

The Company's risk based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include the:

- Purpose of an account or relationship which may influence the assessed risk.
- Level of assets to be deposited by a particular customer or the size of transactions undertaken.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate thata customer not otherwise seen as higher risk should be treated as such.
- Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow the Company to treat the customer as lower risk.
- Level of regulation or other oversight or governance regime to which a customer is subject. A customer that is a financial institution regulated in a country with a satisfactory AML regime poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation. Additionally, companies and their wholly owned subsidiaries that are publicly owned and traded on a recognized exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate and recognized regulatory scheme, which generally pose less risk due to the type of business they conduct and the wider governance regime to which they are subject. Similarly, these entities may not be subject to as stringent account opening due diligence or transaction monitoring during the course of the relationship.
- Regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering perspective.
- Familiarity with a country, including knowledge of local laws, regulations and rules, in addition to the structure and extent of regulatory oversight, as the result of the Company's own operations within the country.
- Use of intermediate corporate vehicles or other structures that have no apparent

commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

Customer risk is also affected by Unusual Activity which may be suspicious:

- Split transactions – the customer is attempting to split a large transactions into several smaller transactions to avoid obligations to provide proof of source of funds
- New customers carrying out large transactions (as opposed to regular customers)
- Customers who cannot provide ID when requested or who provide false ID
- Customers who cannot justify source of funds when requested
- Transactions where customer is accompanied or instructed by another person who tells him what to do

## 2. Risk Mitigation Strategies

The Company has implemented the following risk mitigation strategies:

1. Customer Identification, Due Diligence and Know Your Customer. The Company has implemented a Customer Identification Program (CIP) that enables personnel to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. In general, this program:

1.1. Identifies and verifies the identity of each customer on a timely basis;

1.2. Takes reasonable risk based measures to identify and verify the identity of any beneficial owner;

1.3. Obtains appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions;

1.4. Assesses the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. This due diligence process includes:

1.4.1. A standard level of due diligence that is applied to all customers when initiating or continuing a relationship, such as:

1.4.1.1. Evaluating the nature of the relationship. As an example, determining the length of a customer's relationship with the Company, the products and services provided to a customer, and the manner in which a customer was referred to the Company. The nature of a customer's relationship may serve to mitigate or to increase the overall risk indicators described below.

1.4.1.2. Identifying high risk geographies, including customers located in or conducting business transactions in High Risk Money Laundering and Related Financial Crime Areas; and

1.4.1.3. Identifying high risk entities, banking functions and transactions (refer to the High Risk Entities subtopic below).

1.4.2. The standard level being reduced in recognized lower risk scenarios, such as:

1.4.2.1. Publicly listed companies subject to regulatory disclosure requirements;

1.4.2.2. Other financial institutions (domestic or foreign) subject to an AML regime consistent with all AML recommendations;

1.4.2.3. Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds; or

1.4.2.4. Transactions involving the minimum amounts for particular types of transactions

1.4.3. The standard level being increased with respect to customers that are determined to be of higher risk due to the nature of their activities which may require increased monitoring. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as correspondent Company in relationships. These enhanced duediligence procedures include, but are not limited to:

1.4.3.1. Increased awareness by Company personnel of higher risk customers and transactions within business lines across the Company;

1.4.3.2. Increased levels of the Company's CIP, Know Your Customer (KYC), and enhanceddue diligence;

1.4.3.3. Appropriate additional documentation is obtained to confirm the identity and lawful business activities of a customer;

1.4.3.4. Escalation for approval of the establishment of an account or relationship;

1.4.3.5. An understanding of the normal and expected transactions of a customer, including increased monitoring of transactions;

1.4.3.6. Increased levels of ongoing controls and frequency of reviews of relationships; and

1.4.3.7. Reporting of suspicious activities in compliance with existing reporting requirements.

2. Refer to the Customer Identification Program Policy and Know Your Customer Policy topics of this policy for detailed guidance.

2.1. Monitoring of Customers and Transactions. The degree and nature of monitoring performed by the Company is based upon its size, the AML risks that the Company has identified, the monitoring method being utilized (manual and/or automated), and the type of activity under scrutiny. Not all transactions or customers are monitored in the same way.

2.2. The degree of monitoring is based on the perceived risks associated with a customer, the products or services being used by the customer, and the location of the customer and the transactions. In any respect, such monitoring is appropriately documented. The principal of the Company's risk based monitoring system is to respond to enterprise wide issues based on the Company's analysis of its major risks. Monitoring under this risk based approach allows the Company to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose are reviewed on a regular basis to determine adequacy for the risk levels established. In addition, adequacy of any systems and processes are assessed on a periodic basis by Senior Management and appropriately documented. Refer to the appropriate topics of this policy for detailed guidance with respect to the monitoring of customers and transactions.

2.3. Suspicious Transaction Reporting. The regulatory and legal requirement to report suspicious transactions or activity by the Company provides federal authorities the ability to utilize such financial information to combat money laundering, terrorist financing and other financial crimes. When a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made by the Company. Therefore, a risk based approach for the reporting of suspicious activity under these circumstances is not applicable.

2.4. However, a risk based approach is appropriate for the purpose of identifying suspicious activity (such as directing additional resources at those areas the Company has identified as higher risk). In the same respect, the Company uses information provided by state and federal authorizes to enhance its approach for identifying suspicious activity. In addition, Management should always periodically assesses the adequacy of the Company's system employees training and assessment for identifying and reporting suspicious transactions.

2.5. Training and Awareness. The Company provides its employees with AML Program training that is appropriate and proportional with regard to money laundering and terrorist financing for their respective positions. This enterprise wide effort provides all relevant employees with general information on AML laws, regulations and internal policies that is:

2.5.1. Tailored to the appropriate staff responsibility (e.g. customer contact or operations);

2.5.2. At the appropriate level of detail (e.g. complicated products or customer managed products);

2.5.3. At a frequency related to the risk level of the business line involved; and

2.5.4. Tested to assess knowledge commensurate with the detail of information provided.

## 3. Non-acceptable customers

**Prohibition of anonymous accounts**

Lotus Mao Payments Ltd. does not maintain anonymous accounts or accounts in fictitious names for any new or existing customer.

**Prohibition of shell banks**

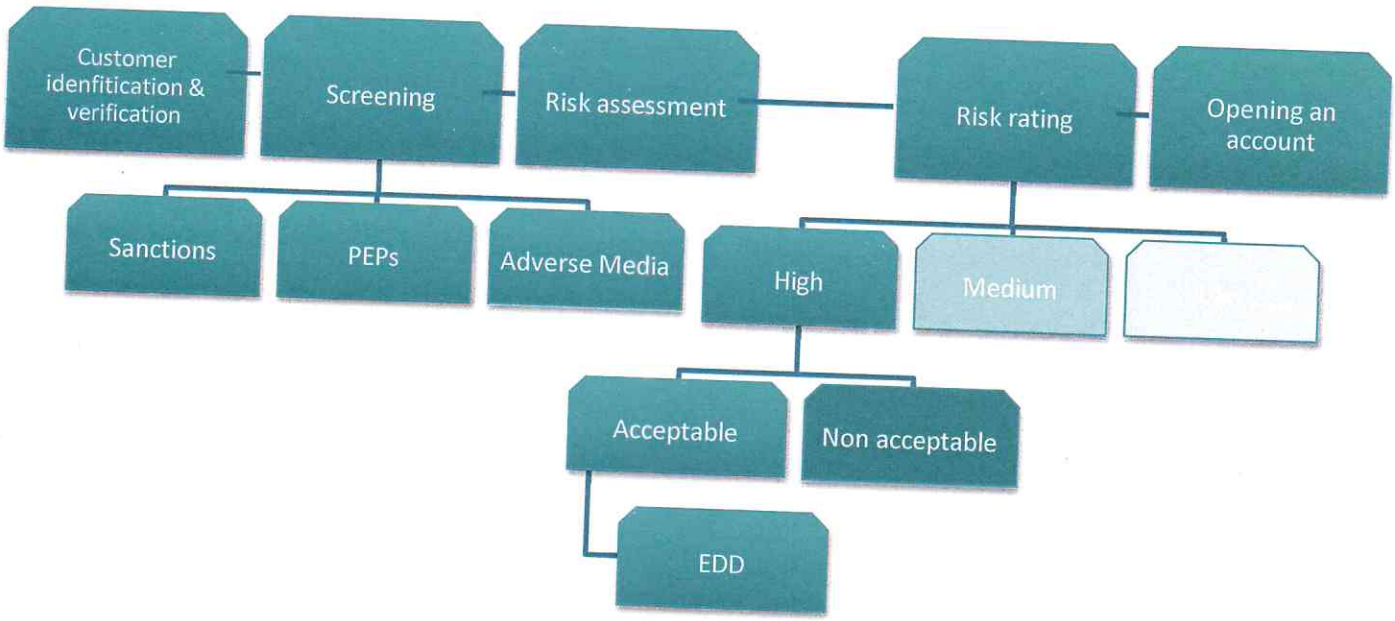
Lotus Mao Payments Ltd. does not maintain correspondent relationships with shell banks, which are defined as non-resident banks that have no permanent executive bodies in the countries in which they have been registered, and has not entered into correspondent relationships with banks that allow their accounts to be used by shell banks.

**A full list of prohibited products and services is provided in Appendix 1.**

# Customer due diligence (CDD/KYC)

Customer due diligence (CDD) is central to an effective anti-money laundering and counter-terrorism financing (AML/CTF) regime. Lotus Mao Payments Ltd. takes measures to identify and verify each of its customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.




The Lotus Mao Payments Ltd. has implemented a KYC program to ensure all kinds of customers (natural or legal persons or legal structures) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented throughout all Lotus Mao Payments Ltd. divisions. The purpose of this is to reduce the risk of the Lotus Mao Payments Ltd. being used for money laundering and financing of terrorism.

Multiple online directories of individual and business information are used to check all customer details before a full Business e-account is activated.

For Business clients we also check their details against the public business registers (for example BUSINESS REGISTERS OF THE PROVINCES AND TERRITORIES).

In all cases, prior to taking on a new customer or engaging in a transaction with a customer with whom we do not have well-established relationship, the Lotus Mao Payments Ltd. completes sufficient due diligence to have confidence in the integrity of the customers and the lawfulness of the proposed transaction by following actions:

1. Make reasonable efforts to determine the true identity of all beneficial ownership of customers.
2. Determine the customer's business addresses, occupation or type of business. Where appropriate, obtain supporting documentation.
3. Inquire whether the customer will have the sole interest in the account or whether there will be other persons who will have access to it. Verify the identity of all such persons and engage in any necessary due diligence regarding such other persons.
4. Customer :

- Determine the legal status (e.g., corporation, partnership or other form of entity).
- Determine whether the customer is regulated, either in Canada or a foreign country.
- Determine all principal persons of the customer, such as officers and directors, or persons who have a substantial beneficial interest (i.e. own equal or more than 25% share in the company). As per the PCMLTFA Regulations, Lotus Mao Payments Ltd. ensures that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership. This includes details of beneficial interests held.
- Obtain copies of all relevant organizational documents:

After the pre-approval to process is given, an employee collects via e-mail and forward to the Lotus Mao Payments Ltd. Compliance Team and Acquirer Bank the full documentation package:

Company registration documents issued in the country where the merchant is incorporated (e.g. Certificate of Registration, Articles and Memorandum, Certificate of Registered Address, Certificate of Directors, etc

Documents stating the ownership rights of the ultimate beneficial owner (e.g. Shareholder Certificate, Share Transfer, eRegister, etc)

Identification documents with the holder's signature (e.g. ID Card, Passport, Driving License, etc.)

Documents stating the rights to represent a company (e.g. Power of Attorney, Articles, Minutes of Meeting etc.)

Agreements with partners and suppliers, if applicable;

License, if applicable;

Financial statements, if applicable;

Processing history, if applicable.

5. Identify the source of the customer's funds.

6. Screen the customer for:

Matches under: Consolidated Canadian Autonomous Sanctions List (under UNA, SEMA or JVCFOA), United Nations Security Council Consolidated List (UN); the US sanctions lists maintained by OFAC (inc. SDN, SSI, CAPTA, NS-MBS and other lists); Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions; OFSI's Consolidated List of Financial Sanctions Targets in the UK; other sanctions lists maintained by G7 member countries;

Matches for jurisdictions listed on the Financial Action Task Force ("FATF"), NCCT list and the FinCEN advisory list;

Persons with significant holding, that hold over 25% equity or more in a business are subject to AML/CTF screening;

Sanctions match. Sanctions and PEP screening is carried out for both legal entities and individuals using WebShield vendor (https://www.webshield.com/); WebShield uses the MemberCheck database (https://membercheck.com/), MemberCheck is a world-renowned provider of specialized databases.

7. Where appropriate, obtain information regarding the frequency with which the customer

expects to transfer funds to or from the account, i.e. monthly, quarterly, or the nature of any third-party payments to or from the account;

8. Where appropriate, obtain and contact reputable references, such as professionals and other members of the financial industry, banks, securities companies, etc.

9. Government Officials and Foreign Bank Accounts.

Special procedures apply for accounts for the benefit of politically exposed persons (PEPs), including senior government and political figures, particularly from certain countries, and for accounts opened by or through foreign banks and for clients from countries or industries deemed high risk. The Lotus Mao Payments Ltd. performs enhanced due diligence and on-going due diligence measures proportionate with the risk of the customer. High risk customers will therefore be subject to enhanced due diligenceand on-going due diligence. On-going due diligence processes will be applied to all existing customers within a specific period that will be determined by whether they are defined as high, medium or low.

In as much as this is not a regular part of the Company's business, you must consult the Compliance Officer before opening any account of this type.

***Please note that currently Lotus Mao Payments Ltd. is not transacting with any PEPs.***

Accounts through an Intermediary;

10. Where accounts come through an intermediary, the Agent must either perform due diligence with respect to the account or satisfy itself that the intermediary has performedthe type of due diligence with respect to the account that would satisfy the Agent's "Know Your Customer" policy.

- The scope of this due diligence will vary depending upon the Agents historical relationship with the intermediary, whether the intermediary is itself a regulated entity and the jurisdiction in which the intermediary is located. The Compliance Officer should be consulted as to the type of due diligence necessary for a specific intermediary.
- At a minimum, due diligence of an intermediary should include a review of the intermediary's anti-money laundering and counter terrorism financing procedures. Where appropriate, representations from the intermediary as to its compliance with its procedures may be obtained.
- Generally speaking, except for intermediaries who are regulated in an appropriate jurisdiction or are well-known by the Agent to have proper anti-money laundering and counter terrorism financing procedures in place, you should perform reference checks

through published sources and others.

11. Counterparties;

The same rules set out in item 10 above also apply to transactions with counterparties on behalf of our customers. For this purpose, counterparties include private transaction counterparties and banks and other dealers, agents and intermediaries. While a relatively low level of due diligence will be required for counterparties who are regulated within a country known to have appropriate and well-enforced anti-money laundering and counter terrorism financing regulations, other counterparties will require the same level of due diligence as clients.

# Enhanced due diligence (EDD)

Lotus Mao Payments Ltd. applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product Lotus Mao Payments Ltd. provides or from a customer of Lotus Mao Payments Ltd.

What the enhanced due diligence actually entails will be dependent on the nature and severity of the risk.

## 1. High-risk situations

In any situation that by its nature presents a higher risk of ML/TF, Lotus Mao Payments Ltd. takes additional measures to mitigate the risk of ML/TF.

Additional measures or EDD may include:

- obtaining additional information on the customer (e.g. connected parties, accounts or relationships) and updating more regularly the customer profile including the identification data;
- obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity), the source of wealth and source of funds;
- obtaining the approval of senior management to commence or continue the relationship; and
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

## 2. Politically Exposed Persons (PEPs)

In order to reduce possible risks Lotus Mao Payments Ltd. conducts EDD at the outset of the business relationship and ongoing monitoring where it knows or suspects that it has business relationship with a PEP.

The definition of 'PEP' is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions
- Is an immediate family member of such a person
- Is a known associate of such a person
- Is resident outside or within the
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by

- Any state;
- The European Community; or
- An international body; or
- An immediate family member or a known close associate in cases where PEP is identified:

- Senior management approval should always be sought before establishing a business relationship with a PEP
- The source of funds should be established

The business relationship should be subject to enhanced and constant monitoring.

It is important that before a business relationship is entered into with a PEP their source of funds is established and Company is satisfied that there are no indications that funds that will be used for transactions to be carried out are derived from corruption (i.e. receipt of bribes), fraud or an attempt by the PEP to remove/hide assets from their homecountry. The source of the PEP's funds may be established by asking the individual concerned a series of questions to determine from where they receive their money. These questions could include confirmation of the main source income (i.e. salary), any business interest or investments from which funds are/will be received.

In order to satisfy itself, below are areas on which questions can be asked of the PEP to determine whether a business relationship should be established- information from this can be presented to Senior Management of Lotus Mao Payments Ltd. for them to make an informed decision:

- What is the position and the duties of the PEP- (please note that a less 'senior' PEP is less of a risk than heads of states, MP's, members of the Judiciary, Ambassadors)
- Are there any family members/close associates that are also PEPs Identify the customer
- and the beneficial owner of the account.
- Know the customer's country of residence.
- Know the objective of opening the account and the volume and nature of the activity expected for the account.
- Obtain information on the occupation and the other income sources.
- Obtain information about the direct family members or associates who have the power to conduct transactions on the account.

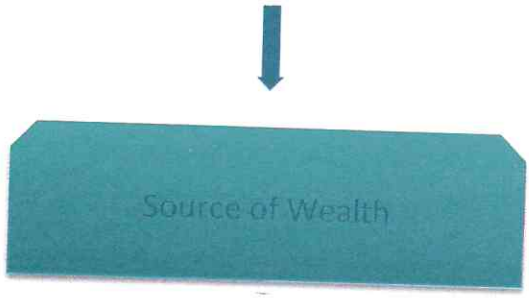
***Please note that currently Lotus Mao Payments Ltd. is not transacting with any PEPs.***

## 3. Source of Wealth vs Source of Funds

Establishing the customer's source of wealth or source of funds is a core requirement of EDD. Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although Lotus Mao Payments Ltd. may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

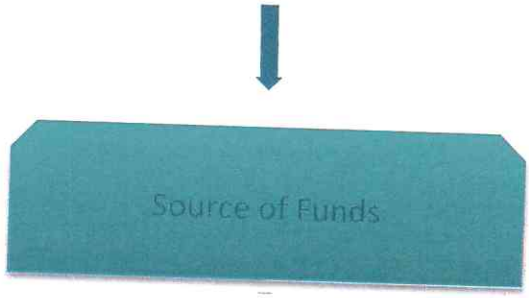
Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and Lotus Mao Payments Ltd. (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

At the beginning of the business relationship




The economic activity generating the total net worth of the customer

As part of the ongoing monitoring process




The activity, event, business, occupation or employment from which funds used in a transaction originate

# On-going monitoring

Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CTF systems. The extent of monitoring is linked to the risk profile of the customer which has been determined through the risk assessment procedures and is dedicated to regularly reassess clients and their transactions to make sure their suspicion level remains justified. Company applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk.

## 1. Risk-based approach to monitoring

Lotus Mao Payments Ltd. takes additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring.

### Monitoring of customers

Lotus Mao Payments Ltd. continuously monitors its business relationship with acustomer by:
• Reviewing client's profile at frequency defined by the client's risk category to ensure that they are up-to-date and relevant;
• monitoring the activities of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may
be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that
is being delivered;

### Transaction monitoring

Lotus Mao Payments Ltd. conducts an on-going transaction monitoring on a risk-based approach and considers:

• the nature and type of transactions (e.g. abnormal size or frequency);
• the nature of a series of transactions;

- the amount of any transactions;
- the geographical origin/destination of a payment;
- the customer's normal activity or turnover.

Lotus Mao Payments Ltd. is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of a customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

Where the basis of the business relationship changes significantly, Lotus Mao Payments Ltd. carries out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures take account of the above changes.

## 2. Methods and procedures

Transaction Monitoring is performed by internally developed Risk Control System (RCS), that covers 24/7 Sanction, PEP Screening as well as prevention of fraud scenarios and detection of suspicious transactions, identification of operational risks, control of breakdowns, responding to and recovering from incidents; review, testing and improvement of Risk Management Framework. RCS collects and analyzes such data as IP address, operation type, Customer ID etc.

When considering how best to monitor customer transactions and activities, Lotus Mao Payments Ltd. takes into account the following factors:

- the size and complexity of its business;
- its assessment of the ML/TF risks arising from its business;
- the nature of its systems and controls;
- the monitoring procedures that already exist to satisfy other business needs;
- the nature of the products and services (which includes the means of delivery or communication).

Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, Lotus Mao Payments Ltd.

examines the background and purpose, including where appropriate, the circumstances of the transactions. The findings and outcomes of these examinations shall be properly documented in writing and be available to assist the relevant authorities, other competent authorities and auditors.

Lotus Mao Payments Ltd. takes the four steps systemic approach to suspicious activity identification:

- Screening
- Asking
- Finding out
- Evaluating

**Screening**

The recognition of an indicator of suspicious activity is the first step in the suspicious activity identification system. The following are some of the suspicious activity indicators most commonly associated with money laundering:

1. Large or frequent transaction.

2. Suspicious activity based on transaction pattern, i.e. a period of significantly increased activity amid relatively dormant periods;

Involvement of one or more of the following entities which are commonly involved in money laundering:

• shelf or shell companies;
• company registered in a known "tax haven" or "off-shore" financial center; • money service operator;
• casino.

3. Currencies, countries or national of countries, commonly associated with international crime or drug trafficking or identified as having serious deficiencies in their anti-money laundering regimes.

4. Customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.

5. Activity is incommensurate with that expected from the customer considering the information already known to you about the customer and the customers previous financial activity.

6. Countries or nationals of countries, commonly associated with terrorist activities or the persons or organizations designated as terrorists or their associates.

7. International and Politically Exposed Persons (PEPs).

**Asking**

In case a transaction or transactions of a customer bear one or more suspicious activity indicators, Lotus Mao Payments Ltd. shall ask the customer questions on the reason for conducting the transaction and the identity of the source and ultimate beneficiary of the money being transacted. Lotus Mao Payments Ltd. also considers whether the customer's story amounts to a reasonable and legitimate explanation of the activity observed. If not, then the customer's activity is regarded to be suspicious and a suspicious transaction report should be made.

**Finding out**

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, when a customer receives "structured" remittances from overseas. Lotus Mao Payments Ltd. can question the customer on the reason for receiving numerous remittances within a short period of time on the grounds that one larger remittance would be quicker, cheaper for the sender to send, and less time consuming for the recipient to handle.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true. If a customer is unwilling, or refuses, to answer questions or gives replies which Lotus Mao Payments Ltd. suspects are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

**Evaluating**

The final step in the suspicious activity identification system is the decision whether or not to make an suspicious transaction report (STR). Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which an STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker,

i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, Lotus Mao Payments Ltd. finds the activity genuinely suspicious then an STR should be made.

# Suspicious transactions reporting

The following list provides several types of behavior or activity that may be suspicious:

- The customer wishes to engage in transactions that lack business sense or are inconsistent with the client's stated business/strategy.
- Upon request, the customer refuses to identify or fails to indicate a legitimate source for his funds.
- A large number of operations in a short time period
- A large number of small operations (crushing)
- Transactions on the amount exceeding the limits (LCTR must be submitted to FINTRAC when transaction is $10,000 or more outside Canada or an incoming for $10,000 or more sent from outside Canada in a single transaction for $10,000 or more; or in two or more transfers of less than $10,000 (that total $10,000 or more) if company senior officer knows they were made within 24 consecutive hours of each other by or on behalf of the same individual or entity (24-hour rule))
- The customer exhibits unusual concern for secrecy, particularly with respect to his identity, type of business or dealings with companies.
- The customer exhibits an unusual lack of concern regarding risks, commissions, or transaction costs.
- The customer has difficulty describing the nature of his business.
- The customer is from, or has accounts in, a country identified as a haven for money laundering.
- Customer enters into transactions with counter parties in locations that are unusual for the customer.
- Customer wants to pay transaction fees that exceed the posted fees
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.

If employee identifies suspicious activity, they contact the Nominated Officer who is responsible for issuing a Suspicious Transaction Report through the FINTRAC online

system. The Nominated Officer should also notify senior management.

## 1. Reporting Suspicions

Anti-money laundering processes require a team approach. Money laundering issues are complex. The Nominated Officer of Lotus Mao Payments Ltd. should not attempt to shift through them alone and if the officer becomes aware of any suspicious circumstances, or have any questions, the officer should promptly consult with Compliance Team of Lotus Mao Payments Ltd.

In the situation that an employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible. Staff should use the internal 'Suspicious Transaction Report Form'. The STR contains as a minimum the following information:

- Details and identification data of all parties to the transaction
- The owner of the monies in question
- How the identity of the client was verified
- A full description of the transaction
- Reason for suspicion and supporting evidence
- Details of any assets which are subject to international sanctions

The law states that an individual working in the regulated sector should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the FINTRAC to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company Nominated Officer. Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options: Report the STR on to FINTRAC or RCMP or CSIS.

File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to FINTRAC or RCMP or CSIS;

The Nominated Officer should complete the Nominated Officer STR Resolution form in the event he decides not to make a report to FINTRAC or RCMP or CSIS.

## 2. Annual reporting to the Bank of Canada

Lotus Mao Payments Ltd. is registered as Payment service provider (PSP) that perform retail payment activities must submit an annual report to the Bank of Canada in accordance with the requirements set out in the Retail Payment Activities Act (RPAA) and the Retail Payment Activities Regulations (RPAR).

Lotus Mao Payments Ltd. completes and submits the bank's annual report form available in the PSP Connect portal by March 31 each year.

The annual report form consists of specific questions related to the PSP's compliance with the RPAA and RPAR, including in the areas of:

- operational risk management and incident response framework
- holding and safeguarding of end-user funds
- ubiquity and interconnectedness
- changes to its retail payment activities
- record-keeping practices
- financial metrics
- any other information the bank requires for its supervision of PSPs.

# AML Training and Awareness

The Company provides security controls for the Human Resources department, including background checks for new employees and contractors.

Lotus Mao Payments Ltd.

- provides annual AML training to all employees;
- ensures that its AML training enables its employees to:

- understand the relevant legislation relating to money laundering, including Federal AML legislation;

- understand its policies, procedures, systems and controls related to money laundering and any changes to these;

- recognize and deal with transactions and other activities which may be related to money laundering;

- understand the types of activity that may constitute suspicious activity in the context ofthe business in which an employee is engaged and that may warrant a notification to the Nominated Officer;

- understand its arrangements regarding the making of a notification to the Nominated Officer;

- be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Company;

- understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Company's Nominated Officer and deputy, where applicable; and

- understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions; and

- ensure that its AML training:

- is appropriately tailored to the Company's activities, including its products, services, customers, distribution channels, business partners, level and complexity of its

transactions; and

- indicates the different levels of money laundering risk and vulnerabilities associated with the matters in stated above.

# Record keeping

All records of business transactions are held for at least five years from the date that the business relationship ends.

The purpose of keeping records is to enable law enforcement to reconstruct business transactions; often well after the original business has been concluded. In making and retaining records you should have in mind the need to provide a clear audit trail of the business you have conducted.
A company must take reasonable measures to

- prevent their loss or destruction;
- prevent their falsification;
- detect and correct any inaccuracies contained in them; and
- prevent unauthorized persons from accessing or using the information contained in them

The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements as per the regulations
- The supporting records in respect of the business relationships or occasional transactions that are the subject of customer due diligence measures or on-going monitoring.
- Record of when the first client identification and verification took place, and how.
- Documents justifying exemption from identification, if applicable.

In relation to the evidence of a customer's identity, businesses must keep the following records:

- A copy of the identification documents accepted and verification evidence obtained, or
- References to the evidence of customer's identity.

Transaction and business relationship records (for example, account files, relevant business correspondence and so on) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect customer.

## APPENDIX 1: PROHIBITED PRODUCTS AND SERVICES

The company reserves the right to expand this list by introducing types of business that may be associated with the distribution of weapons, drugs, prohibited content, financing of terrorism, inciting racial and religious war, violation of human rights or other local and international laws.

The company can also refuse a client whose type of business may be considered high risk during KYC checks.

| Business &Services | Description of Prohibited Activity Types |
|---|---|
| Adult Content | Any merchant connected with visual content, such as pornography or violence that is not generally thought to be appropriate for viewing by children. |
| Alcohol sales via Internet | Merchants selling alcohol products via internet, even if the sale of those items is not restricted to the merchant own country of domicile. |
| Chemicals and Allied Products — not elsewhere classified | Wholesale distributors of chemicals and allied products not elsewhere classified. Products for sale are typically used for industrial purposes. Examples include industrial acids, ammonia and alcohol, heavy, aromatic and other chemicals, chlorine, compressed and liquefied gases, detergents, fuel and oil additives, resins, salts, turpentine, sealants, rust proofing chemicals, coal tar products, dry ice, dyestuffs, glue, gelatin, and explosives. |
| Child Pornography | Any merchant who provides products or services associated with actual or suggested child pornography. Includes any merchant or website who uses the following terminology to promote their product: "lolita," "pedo," "pre-teen," or any other terminology that suggests child pornography. |
| Cigarette/electronic cigarette/ Tobacco/ Vape Sales | Merchants that sell cigarettes/electronic cigarette/tobacco/vape via Internet even if the sale of those items is NOT restricted to the merchants own country of domicile. |

| | |
|---|---|
| Counterfeit goods | Merchants selling counterfeit merchandise (well-known brands) or goods where merchants are infringing on intellectual property rights of trade mark owners (including illegal use of games, game keys e.t.c.) |
| Dealers of high-value precious goods and ect. | Businesses involved in the sale of goods of high value. Examples of these businesses include antique dealers, boat and car sales, dealers in precious stones, jewellers. |
| Drug Paraphernalia | Any business whose products are solely intended for aiding the consumption of illegal drugs. |
| Financial and other Pyramid Sales | Includes sales structures where multiple levels of sales people are making money off one another with no real product or a questionable product to sell: income of the first participants of pyramid is paid at the expense of new participants. |
| Fortune tellers | Includes fortune-tellers, tarot card readers, and mystics. |
| Guns, firearms, munitions sale & distribution | Any sale of firearms by any method including production/recycling of explosive and nuclear fuel. |
| Non-prescription drugs such as pharmaceutical wonder drugs e.g. Steroids, diet pills & all Internet drug stores. | Outlets offering nonprescription drugs such as: pharmaceutical wonder drugs e.g. steroids, diets pills, and all Internet drug stores. |
| Political Organizations and parties | Merchants representing the membership organizations that promote the interests of a national, state, or local political party or candidate, including political groups organized specifically to raise funds for a political party or individual candidate. |
| Religious Organizations (excluding nationally recognized religious organizations/faiths) | Religious organizations that provide worship services, religious training or study, and religious activities, including collection of donations. |
| Sexual Encounter/Escort Firms | Any merchant connected with sexual encounter, including escort services, massage parlors, spas, etc., where sexual encounters are permitted. |