# Money Laundering and Terrorist Financing Prevention Policy

January 2026

# Table of Contents

# I. GENERAL INFORMATION

## 1. Legal Entity

This Anti-Money Laundering and Anti-Terrorist Financing Policy (the **"Policy"**) applies to:

> **Multi Asset Solutions Digital Payments Limited**, trading as **MAS Digital** (the **"Company"**), a company registered in **Canada** under company number **BC1370632**, with a registered office at: **600-1285 West Broadway, Vancouver, British Columbia, Canada, V6H 3X8.**
> MAS Digital is registered with the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** as a **Money Services Business (MSB)** under registration number **M22527201**.

## 2. Regulatory Framework

The Company is subject to and complies with:

- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**
- **PCMLTFA Regulations**
- FINTRAC Guidance, Notices, and Interpretation Papers
- **Criminal Code of Canada**
- **United Nations Act**
- Canadian sanctions legislation
- **FATF Recommendations**

## 3. Purpose of the Policy

The purpose of this Policy is to:

- Prevent MAS Digital from being used to facilitate money laundering or terrorist financing;
- Establish internal controls proportionate to the Company's risk profile;
- Ensure compliance with Canadian law;

- Protect the Company, its customers, and the financial system.

### 4. Scope of Application

This Policy applies to:

- All directors and officers;
- All employees and contractors;
- All customers, accounts, transactions, and services;
- All jurisdictions in which the Company operates or provides services.

## II. DEFINITIONS

### 5. Business Relationship

A **Business Relationship** is established when:
a) A customer opens an account with MAS Digital; **or**
b) MAS Digital conducts **two or more transactions requiring identity verification for the same customer within a five-year period**.
Once established, the relationship is subject to **ongoing monitoring**, enhanced scrutiny, and periodic review.

### 6. Customer

Any natural person or legal entity that uses or seeks to use the Company's services.

### 7. Beneficial Owner

A **natural person** who:

- Owns or controls **25% or more** of a legal entity (directly or indirectly);
- Exercises effective control through other means;
- Is a senior managing official when ownership cannot be determined.

For trusts:

- Settlor(s)
- Trustee(s)
- Beneficiaries
- Any person exercising control

## 8. Virtual Currency

A digital representation of value that is not legal tender, can be transferred electronically, and is used as a medium of exchange, store of value, or unit of account.

## 9. Virtual Currency Transaction

Any transfer, exchange, purchase, sale, deposit, or withdrawal involving virtual currency.

## 10. Money Laundering

As defined in section 462.31 of the **Criminal Code of Canada**, including:

- Conversion or transfer of proceeds of crime;
- Concealment or disguise of illicit origin;
- Acquisition, possession, or use of proceeds of crime;
- Attempts or participation in such acts.

## 11. Terrorist Financing

Any act involving the provision or collection of funds for terrorist purposes, as defined under the **Criminal Code of Canada** and international conventions.

## 12. Politically Exposed Person (PEP)

A **Politically Exposed Person (PEP)** is an individual who holds or has held a **prominent public function**, as well as certain individuals connected to them, due to the higher risk that such persons may be exposed to bribery, corruption, or misuse of public funds.

### *12.1. Foreign Politically Exposed Persons*

A **foreign PEP** is an individual who holds or has held a prominent public function on behalf of a foreign state, including but not limited to:

1. Head of state or head of government;
2. Member of the executive council of government or minister;
3. Deputy minister or equivalent rank;
4. Ambassador, attaché, or counsellor of an ambassador;
5. Military officer with a rank of general or above;
6. President of a state-owned company or bank;

7. Head of a government agency;
8. Judge of a supreme court, constitutional court, or other court of last resort;
9. Leader or president of a political party represented in a legislature.

An individual remains a foreign PEP **for life** under the PCMLTFA.

### *12.2. Domestic Politically Exposed Persons*

A **domestic PEP** is an individual who holds or has held a prominent public function in Canada, including:

1. Governor General, Lieutenant Governor, or head of government;
2. Member of the Senate or House of Commons;
3. Member of a provincial legislature;
4. Deputy minister or equivalent;
5. Ambassador or high commissioner;
6. Military officer with a rank of general or above;
7. President of a Crown corporation or state-owned enterprise;
8. Head of a government agency;
9. Judge of a supreme court, appellate court, or other court of last resort;
10. Leader or president of a political party represented in Parliament or a provincial legislature.

An individual ceases to be a domestic PEP **five (5) years** after leaving office.

### *12.3. Heads of International Organizations (HIOs)*

A **Head of an International Organization (HIO)** is an individual who holds or has held a senior leadership role in an international organization established by governments, including:

- Secretary-General, Director-General, President, or equivalent senior official of an international organization.

An individual ceases to be an HIO **five (5) years** after leaving the position.

### *12.4. Family Members of a PEP or HIO*

Family members include:

1. Spouse or common-law partner;
2. Child of the PEP or HIO;

3. Child of the PEP's or HIO's spouse or common-law partner;
4. Parent of the PEP or HIO;
5. Parent of the PEP's or HIO's spouse or common-law partner.

Family members are treated as PEPs or HIOs for the purposes of risk assessment and due diligence.

#### *12.5. Close Associates of a PEP or HIO*

A **close associate** is an individual who is closely connected to a PEP or HIO, including:

1. A person known to have joint beneficial ownership of a legal entity or arrangement with the PEP or HIO;
2. A person who has a close business relationship with the PEP or HIO;
3. A person who is the beneficial owner of a legal entity or arrangement set up for the benefit of the PEP or HIO.

### 13. Suspicious Transaction

A transaction or attempted transaction for which there are **reasonable grounds to suspect** it is related to ML or TF, regardless of value.

## III. GOVERNANCE & ACCOUNTABILITY

### 14. Chief Anti-Money Laundering Officer (CAMLO)

MAS Digital appoints a **Chief Anti-Money Laundering Officer (CAMLO)** as required by the PCMLTFA.

**CAMLO Authority**

The CAMLO:

1. Operates **independently of revenue functions**
2. Has **direct access to the Board**
3. Cannot be overruled on AML decisions without written justification
4. Bears **personal statutory accountability**

### 15. CAMLO Responsibilities

The CAMLO is responsible for:

1. AML/ATF policy approval and maintenance;
2. FINTRAC reporting (STR, LVCTR, TPR);
3. Enterprise-Wide Risk Assessment (EWRA);

4. Employee training;
5. Independent effectiveness review;
6. Regulator communication;
7. Program updates.

# IV. RISK-BASED APPROACH

## 16. Enterprise-Wide Risk Assessment (EWRA)

MAS Digital conducts an EWRA at least **annually**, assessing:

- Customer risk;
- Product and service risk;
- Geographic risk;
- Delivery channel risk;
- Transaction typologies.

EWRA results directly inform:

- CDD levels;
- Monitoring intensity;
- Control design.

# V. CUSTOMER IDENTIFICATION & VERIFICATION

## 17. When Identification Is Required

Identification and verification must occur:

| Scenario | Requirement |
|---|---|
| Account opening | Mandatory |
| Virtual currency transaction ≥ CAD 10,000 | Mandatory |
| 24-Hour aggregated transactions ≥ CAD 10,000 | Mandatory |
| Suspicious activity | Mandatory |
| Doubts about prior data | Mandatory |

## 18. The 24-Hour Rule

Multiple transactions by or for the same person within **24 consecutive hours** must be aggregated.
If the total equals or exceeds **CAD 10,000**, all identification, recordkeeping, and reporting obligations apply **as if a single transaction occurred**.

## 19. Natural Person Identification

Accepted documents include:

1. Passport
2. Driver's licence
3. Government-issued ID with photo

Required information:

1. Full legal name
2. Date of birth
3. Address
4. Photo
5. Document number and expiry

## 20. Legal Entity Identification

Required information:

1. Legal name
2. Business address
3. Incorporation number
4. Ownership structure
5. Directors and officers
6. Beneficial owners

# VI. CUSTOMER DUE DILIGENCE

## 21. Standard CDD

Standard Customer Due Diligence (CDD) is applied to low- and medium-risk customers and includes the following measures:

1. The Company must verify the customer's identity in accordance with applicable identification and verification requirements.
2. The Company must obtain and assess information regarding the purpose and intended nature of the business relationship.
3. The Company must conduct ongoing monitoring of the business relationship to ensure that transactions are consistent with the customer's profile, risk level, and known source of funds.

## 22. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) must be applied in situations where a higher risk of money laundering or terrorist financing has been identified.

1. EDD is required when any of the following circumstances apply:
2. The customer or the beneficial owner is identified as a Politically Exposed Person (PEP) or a Head of an International Organization (HIO).
3. The customer, beneficial owner, transaction, or source of funds involves a high-risk jurisdiction.
4. The customer conducts transactions that are unusual, complex, or lack an apparent lawful or economic purpose.
5. The customer has been classified as high risk based on the Company's risk assessment.

When Enhanced Due Diligence is applied, the Company must implement the following measures:

1. The Company must identify and verify the source of funds and the source of wealth associated with the customer and the relevant transactions.
2. The establishment or continuation of the business relationship must be approved by senior management.
3. The Company must apply enhanced and more frequent ongoing monitoring of the business relationship and transactions to detect and assess suspicious activity.

# VII. TRANSACTION MONITORING

## 23. Monitoring Obligations

MAS Digital employs advanced monitoring tools, including blockchain analysis, to detect and mitigate potential financial crime risks. The monitoring focuses on identifying unusual or high-risk activities in digital transactions. The key areas of monitoring include:

1. Transaction Patterns: MAS Digital analyzes transaction behavior to identify deviations from normal or expected patterns.
2. Velocity and Frequency: The platform monitors the speed and frequency of transactions to detect rapid or repeated activity that may indicate suspicious behavior.

3. Geographic Exposure: Transactions involving high-risk or sanctioned jurisdictions are carefully scrutinized for potential compliance concerns.
4. Structuring Attempts: MAS Digital identifies attempts to split transactions into smaller amounts to evade reporting thresholds.
5. Use of Privacy-Enhancing Technologies: The system monitors for transactions involving anonymizing tools or privacy-focused technologies that may obscure the origin or destination of funds.

By combining traditional risk indicators with blockchain analysis, MAS Digital strengthens its ability to detect suspicious or potentially illicit activity in digital financial transactions.

# VIII. REPORTING TO FINTRAC

## 24. Suspicious Transaction Reports (STR)

1. STRs must be submitted to FINTRAC as soon as practicable after determining that there are reasonable grounds to suspect that a transaction or attempted transaction is related to money laundering or terrorist financing.
2. There is no minimum monetary threshold for submitting an STR; the obligation applies regardless of the transaction amount.
3. STRs must be filed for both completed and attempted transactions.
4. Employees, officers, and representatives of the Company are strictly prohibited from disclosing to the customer or any third party that an STR has been submitted or is being considered, in order to prevent tipping-off.

## 25. Large Virtual Currency Transaction Reports (LVCTR)

Financial institutions are required to file Large Virtual Currency Transaction Reports (LVCTRs) for certain high-value transactions to ensure compliance with anti-money laundering regulations. Key requirements include:

1. Threshold Requirement: LVCTRs must be submitted for any virtual currency transaction equal to or exceeding CAD 10,000.
2. Aggregation: Transactions within a 24-hour period must be aggregated to determine if the reporting threshold has been reached.

3. Customer Information: Reports must include full details of both the sender and the receiver of the virtual currency, ensuring traceability of funds.

These measures help authorities monitor and detect potential suspicious activity in virtual currency transactions.

### 26. Terrorist Property Reports (TPR)

Financial institutions are required to file Terrorist Property Reports (TPRs) to comply with anti-terrorism and anti-money laundering regulations. Key requirements include:

1. Immediate Submission: TPRs must be submitted to the relevant authorities without delay as soon as terrorist-related property or transactions are identified.
2. No Minimum Threshold: Reporting obligations apply regardless of the value of the transaction or asset.
3. Asset Freezing: Institutions must immediately freeze any identified assets linked to terrorist activities in accordance with applicable laws.

These measures are critical to preventing the financing of terrorism and ensuring compliance with regulatory obligations.

## IX. TRAVEL RULE (VIRTUAL CURRENCY)

### 27. Travel Rule Requirements

For virtual currency transfers equal to or exceeding CAD 1,000, MAS Digital is required to collect and transmit detailed information to ensure regulatory compliance. Key obligations include:

1. Originator Information: Collect and verify the full name, address, and account details of the sender.
2. Beneficiary Information: Collect and verify the full name, address, and account details of the recipient.
3. Data Transmission: Ensure that all required information accompanies the transfer to the receiving institution.
4. Record Retention: Maintain all related records for a minimum of five years.

Additionally, all systems and processes must be technically designed to enforce compliance with the Travel Rule.

# X. SANCTIONS COMPLIANCE

## 28. Sanctions Screening

MAS Digital screens all customers and transactions against applicable sanctions lists to prevent prohibited dealings. Key procedures include:

1. Applicable Sanctions Lists: Customers and transactions are screened against the United Nations sanctions list and the Canadian sanctions list.
2. Action on Matches: If a potential match is identified, the institution must immediately freeze the account, notify the relevant regulatory authorities, and prohibit the transaction from proceeding.

These measures are essential for compliance with international and domestic sanctions regulations.

# XI. RECORDKEEPING

## 29. Retention Periods

MAS Digital maintains comprehensive records to comply with regulatory requirements. Standard retention periods are as follows:

1. Identification Records: Maintain for five years from the end of the business relationship.
2. Transaction Records: Maintain for five years from the date of the transaction.
3. Suspicious Transaction Reports (STR), Large Virtual Currency Transaction Reports (LVCTR), and Terrorist Property Reports (TPR): Maintain for five years from submission.
4. Training Records: Maintain for five years from the date of training.

Enhanced Watchlist Risk Assessment (EWRA) Records: Maintain for five years from completion.

# XII. TRAINING & REVIEW

## 30. Employee Training

All MAS Digital employees receive ongoing anti-money laundering and counter-terrorist financing training to ensure regulatory compliance. Key training requirements include:

1. Onboarding Training: Mandatory AML/CFT training for all new employees.
2. Annual Refresher Training: All staff must complete annual updates on AML/CFT regulations.
3. Role-Based Depth: Training content is tailored according to employee roles and responsibilities.
4. Documented Attendance: All training sessions must be formally documented and records retained.

## 31. Effectiveness Review

MAS Digital conducts regular reviews of its AML/CFT program to ensure continued effectiveness. Procedures include:

1. Biennial Reviews: A comprehensive review is conducted at least every two years
2. Independent Assessment: Reviews are performed independently of the AML operations team.
3. Documentation and Remediation: Findings are formally documented and any deficiencies are promptly addressed.

# XIII. FINAL PROVISIONS

## 32. Enforcement

Violations of the AML/CFT policy may result in serious consequences, including:

1. Regulatory Penalties: Fines and sanctions imposed by FINTRAC or other authorities.
2. Criminal Sanctions: Prosecution under applicable criminal laws.
3. MSB Deregistration: Possible loss of registration as a Money Services Business.

4. Personal Liability: CAMLO and senior officers may be held personally liable for non-compliance.

## 33. Policy Review

MAS Digital's AML/CFT Policy is reviewed on an ongoing basis to maintain regulatory compliance and operational relevance. Reviews occur:

1. Annually: To ensure continued alignment with internal policies and regulations.
2. Upon Regulatory Change: When changes in law or regulation require updates.
3. Upon Material Business Change: Whenever there are significant changes in business activities, products, or risk exposure.