ANTI–MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM (AML/CFT) POLICY

Company: FRESCO MODO LIMITED (NZBN: 9429047819740)
Incorporation: New Zealand, 2019
Effective Date: 21 June 2022 (replaced the previous AML Policy dated 19 August 2020)
Approved By: M. Allardice, Director
Review Cycle: Annual or as required by law

---

1. PURPOSE AND OBJECTIVES

This Anti–Money Laundering and Countering Financing of Terrorism (AML/CFT) Policy ("Policy") sets out the framework, principles, and controls adopted by FRESCO MODO LIMITED ("Fresco Modo", "the Company") to prevent, detect, and deter money laundering (ML), terrorism financing (TF), and related financial crimes.

The objectives of this Policy are to:

- Ensure full compliance with the **Anti-Money Laundering and Countering Financing of Terrorism Act 2009 of New Zealand (AML/CFT Act)** and its amendments, regulations, and applicable guidance.
- Protect the Company from being misused for money laundering, terrorism financing, proliferation financing, fraud, sanctions evasion, or other illicit activities.
- Establish a robust risk-based AML/CFT compliance framework across all business lines.
- Define roles, responsibilities, and accountability for AML/CFT compliance.
- Promote a strong culture of compliance, integrity, and ethical conduct.

This Policy applies to all directors, officers, employees, contractors, agents, and representatives of the Company.

---

2. BUSINESS PROFILE AND RISK CONTEXT

Fresco Modo operates across multiple business lines with international exposure, including:

1. **International Trade Activities**

2. **Financial Services for International Traders**, including factoring and trade finance–related services

3. **Crypto Trading and Digital Asset–Related Activities**

4. **International Logistics and Supply Chain Services**

Given the cross-border nature, involvement with financial flows, trade documentation, digital assets, and third-party intermediaries, the Company recognizes that it is exposed to heightened ML/TF risks. This Policy adopts a **risk-based approach** proportionate to the nature, size, and complexity of the Company's activities.

---

3. REGULATORY AND LEGAL FRAMEWORK

This Policy is guided by, and must be read in conjunction with, the following:

- Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (New Zealand)
- AML/CFT Amendment Acts and Regulations
- Financial Action Task Force (FATF) Recommendations
- Guidance issued by New Zealand supervisors (DIA, FMA, RBNZ, as applicable)
- United Nations Security Council Resolutions on sanctions and terrorism
- Applicable foreign AML/CFT and sanctions laws where the Company operates

Where conflicts arise between jurisdictions, the Company applies the higher standard.

---

4. AML/CFT GOVERNANCE STRUCTURE

4.1 Director

The Director has ultimate responsibility for AML/CFT compliance and shall:

- Approve this Policy and material amendments
- Oversee the effectiveness of the AML/CFT framework
- Ensure adequate resources are allocated to AML/CFT compliance
- Receive regular AML/CFT reporting

4.2 AML/CFT Compliance Officer

The Company shall appoint a qualified **AML/CFT Compliance Officer**, responsible for:

- Implementing and maintaining the AML/CFT Programme
- Conducting and updating the AML/CFT Risk Assessment
- Monitoring compliance with this Policy and applicable laws
- Reporting suspicious activities to the New Zealand Financial Intelligence Unit (FIU)
- Acting as the primary liaison with regulators and law enforcement

4.3 Senior Management

Senior management shall:

- Support the Compliance Officer
- Embed AML/CFT controls within business operations
- Ensure staff adherence to this Policy

4.4 Employees and Representatives

All employees and representatives must:

- Comply with AML/CFT obligations
- Complete required AML/CFT training
- Promptly report suspicious activity

---

5. RISK-BASED APPROACH

Fresco Modo adopts a **risk-based approach (RBA)** to AML/CFT compliance, ensuring that higher-risk activities receive enhanced scrutiny.

5.1 AML/CFT Risk Assessment

The Company maintains a documented AML/CFT Risk Assessment covering:

- Customer risk
- Geographic risk
- Product and service risk
- Delivery channel risk

The Risk Assessment is reviewed at least annually or upon material changes to the business.

5.2 Risk Categories

Customers and transactions are categorized as:

- Low Risk
- Medium Risk
- High Risk

Controls are applied proportionately.

---

6. CUSTOMER DUE DILIGENCE (CDD)

6.1 When CDD Is Required

CDD must be conducted when:

- Establishing a business relationship
- Conducting an occasional transaction above regulatory thresholds
- Suspicion of ML/TF arises
- There are doubts about previously obtained information

6.2 Standard CDD

Standard CDD includes:

- Identification and verification of the customer
- Identification of beneficial owners
- Understanding the nature and purpose of the business relationship

6.3 Enhanced Due Diligence (EDD)

EDD is required for higher-risk situations, including:

- Politically Exposed Persons (PEPs)
- High-risk jurisdictions
- Complex ownership structures
- Crypto-related activities

EDD measures may include source of funds/wealth verification and senior management approval.

6.4 Simplified Due Diligence

Simplified CDD may be applied where permitted by law and justified by low risk.

---

7. BENEFICIAL OWNERSHIP

The Company identifies and verifies all beneficial owners in accordance with the AML/CFT Act, ensuring transparency of ownership and control structures.

8. POLITICALLY EXPOSED PERSONS (PEPs)

Fresco Modo applies enhanced scrutiny to PEPs, including:

- Screening at onboarding and periodically thereafter
- Senior management approval
- Ongoing monitoring

9. SANCTIONS AND TERRORIST DESIGNATIONS

The Company screens customers, counterparties, and transactions against applicable sanctions and terrorist designation lists.

Any matches must be escalated immediately to the Compliance Officer.

10. TRANSACTION MONITORING

FRESCO MODO LIMITED (the “Company”) maintains a comprehensive, risk-based transaction monitoring framework designed to identify, assess, and escalate unusual, complex, or suspicious activity across all business lines. The framework is proportionate to the Company’s size, nature, and risk exposure and reflects the multi-jurisdictional and multi-product nature of its operations, including international trade, financial services, crypto trading, and logistics.

Transaction monitoring is a core component of the Company’s AML/CFT Programme and operates in conjunction with customer due diligence, risk assessment, and ongoing customer monitoring.

10.1 Objectives of Transaction Monitoring

The objectives of transaction monitoring are to:

- Detect unusual or suspicious transactions or patterns that may indicate money laundering, terrorism financing, proliferation financing, sanctions evasion, fraud, or other financial crime
- Ensure transactions are consistent with the Company’s knowledge of the customer, including their business activities, risk profile, source of funds, and expected transactional behaviour
- Identify emerging risks through behavioural and trend analysis
- Enable timely investigation, escalation, and external reporting where required by law

10.2 Scope of Transaction Monitoring

Transaction monitoring applies to all transactions conducted by or through the Company, including but not limited to:

- Payments and receipts related to international trade activities
- Cash flows arising from factoring and trade finance–related services
- Fiat and crypto asset transactions, including conversions and transfers
- Payments associated with international logistics, freight, and supply chain services
- Transactions involving third parties, intermediaries, agents, or settlement partners

Monitoring covers both **single transactions** and **aggregated transactional behaviour over time**.

10.3 Risk-Based Monitoring Approach

The Company applies transaction monitoring on a risk-sensitive basis, taking into account:

- Customer risk rating (low, medium, high)
- Product and service risk
- Geographic and jurisdictional exposure
- Delivery channels and use of intermediaries
- Historical transactional behaviour

Higher-risk customers, transactions, and jurisdictions are subject to enhanced monitoring, increased frequency of review, and lower tolerance thresholds.

10.4 Monitoring Methods and Controls

The Company employs a combination of **automated, rule-based, and manual controls**, which may include:

- Threshold-based alerts for high-value or unusual transactions
- Velocity monitoring to identify rapid movement of funds or assets
- Pattern recognition to detect structuring, layering, or circular transactions
- Comparison of actual transactions against expected activity established at onboarding
- Periodic sampling, thematic reviews, and post-event analysis

Monitoring rules and parameters are reviewed regularly to ensure ongoing effectiveness.

10.5 Trade and International Commerce Monitoring

To mitigate trade-based money laundering (TBML) risks, the Company applies enhanced monitoring to international trade transactions, including:

- Review of trade documentation such as invoices, contracts, bills of lading, packing lists, and certificates of origin
- Consistency checks between goods description, quantity, pricing, Incoterms, and shipment routes
- Identification of over-invoicing, under-invoicing, duplicate invoicing, or fictitious trade
- Monitoring of unusual trade routes, transshipment points, or high-risk ports
- Enhanced scrutiny of counterparties with limited operating history or opaque ownership structures

---

10.6 Factoring and Financial Services Monitoring

For factoring and trade finance–related services, transaction monitoring includes:

- Verification that financed invoices correspond to genuine underlying commercial transactions
- Monitoring repayment flows for consistency with contractual terms and commercial logic
- Identification of early, late, accelerated, or third-party repayments without clear explanation
- Detection of repeated refinancing of the same invoices or circular financing structures
- Monitoring for sudden changes in transaction volume, jurisdictions, or counterparties

---

10.7 Crypto Asset Transaction Monitoring

Given the heightened inherent risks associated with crypto assets, the Company applies enhanced transaction monitoring measures, including:

- Monitoring of customer- and counterparty-associated wallet addresses
- Screening of crypto transactions for exposure to high-risk typologies such as mixing services, tumblers, privacy-enhancing technologies, darknet marketplaces, or sanctioned addresses

- Review of unusually large, rapid, or complex crypto transfers inconsistent with the customer profile
- Monitoring of fiat-to-crypto and crypto-to-fiat conversions for legitimacy and economic rationale
- Enhanced scrutiny of transactions involving high-risk or unregulated virtual asset service providers (VASPs)

Where feasible, blockchain analytics tools or reliable third-party intelligence sources may be used to support monitoring activities.

10.8 Geographic and Jurisdictional Monitoring

Transactions involving higher-risk jurisdictions are subject to enhanced scrutiny, including those involving:

- Countries identified by FATF as high-risk or under increased monitoring
- Jurisdictions subject to international sanctions or embargoes
- Countries known for high levels of corruption, weak AML/CFT regimes, or significant financial crime risk

---

10.9 Ongoing Behavioural Monitoring

The Company conducts ongoing monitoring of customer behaviour to identify:

- Material deviations from expected transactional patterns
- Sudden changes in business model, ownership structure, or source of funds
- Inconsistent, incomplete, or evasive explanations for transactions
- Repeated transactions structured to avoid reporting or internal thresholds

Where increased risk is identified, customer risk ratings are updated accordingly.

10.10 Alert Review, Investigation, and Escalation

All alerts and identified unusual activity must be:

- Reviewed promptly by appropriately trained personnel
- Analysed using available customer, transactional, and contextual information
- Documented with clear rationale, findings, and conclusions

Where suspicion cannot be reasonably resolved, the matter must be escalated to the AML/CFT Compliance Officer without delay.

10.11 Determination and Reporting of Suspicious Activity

Where, following reasonable inquiry, a transaction or pattern of activity gives rise to suspicion of money laundering or terrorism financing:

- The activity must be reported internally immediately
- The AML/CFT Compliance Officer shall determine whether a Suspicious Activity Report (SAR) is required
- External reporting shall be made to the appropriate authority in accordance with statutory requirements and timeframes

Under no circumstances shall customers or third parties be informed that a SAR has been made or is being considered.

10.12 Record Keeping and Audit Trail

The Company maintains complete and accurate records relating to transaction monitoring, including:

- Alerts generated and reviews conducted
- Investigations performed and decisions taken
- Internal and external reports submitted

Such records form part of the Company's AML/CFT audit trail and are retained for a minimum of five (5) years in accordance with legal requirements.

---

11. SUSPICIOUS ACTIVITY REPORTING

11.1 Internal Reporting

Employees must immediately report suspicious activity to the Compliance Officer.

11.2 External Reporting

The Compliance Officer shall submit Suspicious Activity Reports (SARs) to the New Zealand FIU without tipping off the customer.

---

12. RECORD KEEPING

The Company retains AML/CFT records for at least **five (5) years**, including:

- CDD documentation
- Transaction records
- Risk assessments

- Training records

---

13. CRYPTO ASSET–SPECIFIC CONTROLS

Given the inherent risks associated with crypto assets, Fresco Modo applies:

- Enhanced onboarding procedures
- Blockchain transaction analysis where feasible
- Restrictions on privacy-enhancing technologies
- Ongoing monitoring of wallet activity

---

14. TRADE-BASED MONEY LAUNDERING (TBML) CONTROLS

The Company implements controls to mitigate TBML risks, including:

- Verification of trade documents
- Pricing and quantity checks
- Counterparty due diligence
- Monitoring of unusual shipping routes

---

15. FACTORING AND TRADE FINANCE CONTROLS

For factoring and related financial services, the Company applies:

- Verification of underlying invoices
- Assessment of commercial rationale
- Monitoring of repayment flows

---

16. TRAINING AND AWARENESS

All employees receive AML/CFT training:

- Upon onboarding
- Annually thereafter
- When laws or risks change

Training is tailored to roles and responsibilities.

---

17. INDEPENDENT AUDIT AND REVIEW

The AML/CFT Programme is subject to independent audit at least every two years or as required by law.

Findings are reported to the Director and addressed promptly.

---

18. BREACH MANAGEMENT AND DISCIPLINARY ACTION

Breaches of this Policy may result in disciplinary action, including termination of employment and reporting to authorities.

---

19. CONFIDENTIALITY AND DATA PROTECTION

All AML/CFT information is handled confidentially and in accordance with applicable privacy laws.

---

20. POLICY REVIEW AND MAINTENANCE

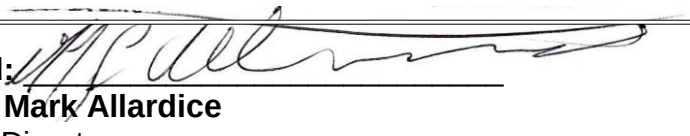
This Policy is reviewed annually and updated to reflect:

- Regulatory changes
- Business developments
- Emerging ML/TF risks

---

21. Director APPROVAL

This AML/CFT Policy is approved by the sole Directors of FRESCO MODO LIMITED and is effective as of the date stated above.

Signed: 
Name: Mark Allardice
Title: Director
Date: 21 June 2022