ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING PROGRAM

CoinPort Pty Ltd (trading as CoinPort Exchange)

AUSTRAC Registration:

- Virtual Asset Service Provider (VASP) - formerly Digital Currency Exchange (DCE)
- Registered Digital Currency Exchange Number: 100633359
- Registered Independent Remittance Dealer Number: IND100633359-001
- Registration Date: 03 February 2020
- AUSTRAC Account Number (AAN): 100633359
- Legal Name: CoinPort PTY LTD

Program Version: 3.0 (2026 Unified Program)
Effective Date: 5 January 2026
Next Review Date: February 2026 (initial post-implementation review), then annually each January
AML/CTF Compliance Officer: Nicanor Nuqui

TABLE OF CONTENTS

INTRODUCTION

GOVERNANCE AND OVERSIGHT

MONEY LAUNDERING AND TERRORISM FINANCING

RISK MANAGEMENT

OPERATIONAL REQUIREMENTS

CUSTOMER IDENTIFICATION PROCEDURES

APPENDICES

INTRODUCTION

1. ABOUT THE AML/CTF ACT

1.1 The Anti-Money Laundering ("AML") and Counter-Terrorism Financing ("CTF") Act 2006 ("AML/CTF Act") and the Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 ("Rules") broad purpose is to regulate financial transactions in a way that will help identify, mitigate and manage money laundering and terrorism financing risks.

1.2 The AML/CTF Act provides general principles and obligations while detailed operating rules are covered in rules made by the Australian Transaction Reports and Analysis Centre ("AUSTRAC"). AUSTRAC is the government agency responsible for administering the AML/CTF Act.

1.3 The AML/CTF Act applies to persons who provide specified services (known as "designated services"). Persons providing designated services are called "reporting entities".

1.4 CoinPort Pty Ltd ("CoinPort") provides one or more designated services listed in the AML/CTF Act and is therefore a reporting entity. These services are included in the AML/CTF Act because they are vulnerable to abuse by criminals for money laundering or terrorism financing purposes.

1.5 The AML/CTF Act adopts a risk-based approach. This approach means that the reporting entity decides how best to identify, mitigate and manage the risk of money laundering and terrorism financing through its business. Reporting entities therefore need to undertake a comprehensive assessment of these risks relative to their businesses.

2. ADOPTION

2.1 CoinPort adopts this unified Program as its AML/CTF Program ("Program") for the purposes of the AML/CTF Act. On and from 5 January 2026, CoinPort must comply with the Program, as varied from time to time.

2.2 This unified Program replaces the previous Part A and Part B structure in accordance with the 2026 AML/CTF reforms, which abolished the requirement to maintain separate program components.

2.3 From 31 March 2026, CoinPort's registration designation changes from "Digital Currency Exchange (DCE)" to "Virtual Asset Service Provider (VASP)" to align with international Financial Action Task Force (FATF) standards. This terminology change reflects the expanded scope of regulated virtual asset services.

VERSION	DATE	NOTES
1.0	6 June 2021	Original Part A and Part B prepared
2.0	1 July 2024	Edits for fraud prevention
3.0	5 January	Unified program for 2026 compliance

	2026	including Travel Rule; DCE→VASP terminology transition

2A. 2026 REFORMS: COINPORT'S RISK-BASED APPROACH

2A.1 Overview of 2026 Regulatory Changes

The 2026 AML/CTF reforms represent a fundamental shift from prescriptive, rules-based compliance to an outcomes-focused, risk-based approach. CoinPort's Program is designed to demonstrate effective management of money laundering, terrorism financing, and proliferation financing risks specific to our business operations, rather than simply meeting checklist requirements.

2A.2 Key Reforms Affecting CoinPort

From Prescriptive to Outcomes-Based:

- Previous framework: Detailed Part A/Part B requirements with prescribed procedures
- New framework: Unified program demonstrating effective risk management outcomes
- Focus: What CoinPort achieves in managing ML/TF/PF risks, not just what procedures we follow

Proliferation Financing Added:

CoinPort must now identify, assess, and mitigate risks related

to Proliferation Financing (PF) - the financing of weapons of mass destruction - alongside money laundering (ML) and terrorism financing (TF). All references to "ML/TF" in this Program are understood to include PF.

Mandatory Risk Assessments:

Risk assessments are no longer "best practice" but an explicit legal obligation. CoinPort must:

- Conduct comprehensive ML/TF/PF risk assessments across all business activities
- Update risk assessments following any "adverse event" or significant business change
- Document risk assessment methodology and findings
- Demonstrate how controls are proportionate to identified risks

Dynamic Program Updates:

Programs must be updated following:

- Any adverse event (regulatory action, significant breach, fraud incident)
- Material changes to business model or services
- Entry into new markets or jurisdictions
- Introduction of new products or delivery channels
- Identification of new or emerging ML/TF/PF risks

2A.3 CoinPort's Specific Risk Profile

CoinPort has assessed its ML/TF/PF risk profile based on our specific business characteristics:

Services Provided:

- Buying, selling, exchanging, and custody of virtual assets
- Focus on major cryptocurrencies (Bitcoin, Ethereum, stablecoins)
- Retail-focused digital currency exchange operations

Customer Types (Risk Level: LOW to HIGH):

- Individual retail customers - Standard retail cryptocurrency users
- Companies and corporate entities - Australian and foreign companies requiring beneficial ownership verification
- Self-Managed Super Funds (SMSFs) - Pension and retirement investment vehicles
- Trusts - Including family trusts, unit trusts, and discretionary trusts
- Partnerships - Business partnerships and joint ventures
- Institutional clients - Superannuation funds, corporate treasury operations
- This diverse customer base requires comprehensive KYC procedures across all entity types (Sections 34-42)
- Enhanced fraud prevention for vulnerable customers (55+ age verification for individuals)

Delivery Channels (Risk Level: MEDIUM):

- Non-face-to-face onboarding (inherent higher risk, mitigated by robust KYC)
- Digital platform with instant payment capabilities (Monoova OSKO/PayID integration)
- Blockchain-based transfers (traceability via AMLBot blockchain analytics and sanctions screening)
- Real-time wallet address screening for sanctioned entities, blacklisted exchanges, and high-risk counterparties

Jurisdictions (Risk Level: LOW to MEDIUM):

- Primary operations: Australia (lower risk, robust AML/CTF framework)
- Secondary focus: Remittance corridors to FATF-compliant jurisdictions
- Sanctions screening against all high-risk jurisdictions
- No business in sanctioned or non-cooperative jurisdictions

Proliferation Financing Risk Assessment:
CoinPort's PF risk is assessed as **LOW-MEDIUM** due to:

- Diverse customer base including corporate entities (increased complexity vs individual-only model)
- Enhanced beneficial ownership verification for all corporate structures
- Comprehensive sanctions screening including proliferation-related sanctions

- Transaction monitoring for unusual patterns that could indicate PF activity
- No trade finance or dual-use goods transactions (reduces risk)
- No business relationships with entities in jurisdictions of PF concern

2A.4 CoinPort's Risk-Based Controls

Proportionate Customer Due Diligence:

CoinPort applies three tiers of CDD based on customer risk:

Risk Level	Criteria	CDD Approach
Simplified CDD	ASX-listed companies, APRA-regulated institutions, majority-owned subsidiaries of listed companies, licensed and regulated entities	Simplified verification procedures per Section 35(i), reduced beneficial ownership requirements, annual reviews
Standard CDD	Individual retail customers, Australian standard companies, SMSFs, standard partnerships, simple trusts	Standard KYC verification, annual reviews, automated transaction monitoring
Enhanced CDD	PEPs, high transaction volumes (>$50k/month), cross-border remittances, complex corporate structures, offshore entities, trusts with multiple layers, self-employed with complex income, adverse media hits	Additional source of funds/wealth verification, senior management approval, semi-annual reviews, enhanced monitoring, beneficial ownership to ultimate individual level

Digital Verification Embraced:

- CoinPort utilizes electronic identity verification through approved KYC providers (KYC-AID and Sumsub)
- Liveness detection and document verification technology

- No requirement to maintain physical certified copies in most cases
- Blockchain analytics for transaction verification via AMLBot
- AMLBot real-time screening for sanctioned wallet addresses, blacklisted exchanges, and high-risk counterparties
- Real-time sanctions screening at customer onboarding and daily thereafter

Risk-Triggered Enhanced Due Diligence:
Enhanced CDD is automatically triggered when:

- Customer identified as PEP (domestic, foreign, or international organization)
- Monthly transaction volume exceeds $50,000 AUD
- Complex corporate structure with multiple layers of ownership
- Offshore corporate entities or trusts in secrecy jurisdictions
- Beneficial owners cannot be clearly identified to ultimate individual level
- Company or trust with no clear commercial purpose
- AMLBot blockchain analytics flag high-risk wallet interactions (sanctioned addresses, blacklisted exchanges, mixers)
- Customer based in or transacting with higher-risk jurisdictions
- Unusual transaction patterns detected
- Source of funds unclear or inconsistent with customer profile
- Travel Rule information incomplete or suspicious (from March 2026)

- Cash-intensive business operations
- Significant changes in company ownership or control structure
- AMLBot detects connections to darknet markets, ransomware, or theft
- Deposits from exchanges flagged as non-compliant by AMLBot

2A.5 Strengthened Governance & Oversight (2026Requirements)

Management Accountability:

Senior management must take "reasonable steps" to ensure CoinPort complies with this Program. This includes:

- Regular review of compliance metrics and risk indicators
- Timely response to identified deficiencies
- Adequate resourcing of compliance functions
- Setting appropriate "tone from the top" regarding compliance culture

Compliance Officer Authority:

The AML/CTF Compliance Officer (Nicanor Nuqui) is:

- At management level with direct Board reporting
- Empowered to make compliance decisions independently
- Authorized to halt transactions or refuse customers based on risk
- Responsible for operational implementation of this Program
- Accountable for reporting compliance status to the Governing Body

Governing Body Oversight:
CoinPort's Board receives:

- Monthly compliance reports covering SMRs, risk incidents, and Program effectiveness
- Quarterly risk assessment summaries
- Annual independent review findings
- Immediate notification of adverse events or regulatory contact
- Regular training on ML/TF/PF risks and obligations

2A.6 Reporting Groups (Replacing Designated Business Groups)

Current Status:

CoinPort operates as a single entity and is not part of a Reporting Group.

If CoinPort Forms a Reporting Group:

- CoinPort would appoint a Lead Entity responsible for group-wide compliance
- Lead Entity would coordinate risk assessments across the group
- Enhanced information sharing permitted within the group (subject to updated tipping-off rules)
- Collective risk management approach while maintaining individual entity accountability
- Refer to Section 6 for Reporting Group procedures

2A.7 CoinPort's Five Pillars of Compliance

Pillar 1: Unified Governance Framework

- Program approved by Board of Directors (Section 9)
- AML/CTF Compliance Officer explicitly named with defined authority (Section 10)
- Monthly Board reporting on ML/TF/PF risks and compliance status (Section 9.3)

Pillar 2: ML/TF/PF Risk Assessment

- Comprehensive risk assessment across four categories:
    - Customers: Individuals, companies, trusts, SMSFs, partnerships, and institutional clients, risk-rated low to high
    - Services: Virtual asset exchange, transfer, custody
    - Delivery Channels: Digital platform, blockchain-based
    - Jurisdictions: Australia-focused, limited cross-border
- Dynamic review triggers documented (Section 15.5-15.9)
- Risk Assessment Matrix maintained (Appendix 3)

Pillar 3: Risk-Based Customer Due Diligence

- Simplified CDD for ASX-listed companies, APRA-regulated entities, and majority-owned subsidiaries (Section 35)
- Standard CDD for individuals, standard companies, SMSFs, and simple trusts (Sections 34-36)
- Enhanced CDD triggered by specific risk factors including complex corporate structures, PEPs, and high transaction volumes (Section 30)
- Ongoing Due Diligence (ODD) with customer risk re-assessment, transaction monitoring, and periodic KYC refresh (Section 30)

- Proportionate controls based on actual risk presented throughout customer lifecycle

Pillar 4: Personnel & Culture

- Employee due diligence program (Section 17)
- Risk awareness training program with annual refreshers (Section 18)
- Culture of compliance: Staff empowered to report suspicions without fear
- Understanding of tipping-off laws and harm-based test (Section 22)

Pillar 5: Reporting & Record Keeping

- Travel Rule implementation for VASP-to-VASP transfers (Section 25)
- Clear SMR workflow and decision-making process (Section 22)
- TTR and IVTS reporting procedures (Sections 23-24)
- Seven-year record retention (Section 20)
- Annual independent evaluation (Section 11.2)

2A.8 Demonstrating Effectiveness (Outcomes Focus)

CoinPort demonstrates Program effectiveness through:

Metrics and KPIs:

- SMR submission rate and timeliness
- Transaction monitoring alert quality (false positive rate)
- Customer risk rating accuracy
- Staff training completion rates

- Independent review findings and remediation
- Regulatory feedback and AUSTRAC correspondence

Continuous Improvement:

- Quarterly review of transaction monitoring rules
- Annual review of risk assessment methodology (January each year)
- Post-incident analysis and control enhancements
- Regular testing of Travel Rule systems
- Blockchain analytics tool effectiveness reviews
- Initial post-implementation review (February 2026) to assess Version 3.0 effectiveness

Adverse Event Response:
When an adverse event occurs (breach, fraud, regulatory contact), CoinPort:

1. Immediately documents the event and circumstances
2. Assesses impact on risk assessment and Program adequacy
3. Implements corrective actions within defined timeframes
4. Updates this Program if systematic issues identified
5. Reports to Board with remediation plan
6. Conducts follow-up testing to verify effectiveness

2A.9 CoinPort's Commitment to Risk-Based Compliance

CoinPort commits to:

- Proportionate controls: Resources allocated based on actual risk, not arbitrary rules

- Flexibility: Adapting procedures as risks evolve and business changes
- Effectiveness over compliance: Focus on preventing ML/TF/PF, not just ticking boxes
- Transparency: Clear documentation of risk decisions and rationale
- Continuous improvement: Learning from incidents, near-misses, and industry developments
- Regulatory engagement: Proactive communication with AUSTRAC on risk management approach

This risk-based approach allows CoinPort to:

- Focus resources on highest-risk areas (enhanced monitoring of PEPs, large transactions, cross-border transfers)
- Streamline processes for low-risk customers (standard retail individuals)
- Respond quickly to emerging threats (new ML/TF/PF typologies, sanctions developments)
- Demonstrate compliance through outcomes, not just documentation
- Maintain business efficiency while managing risk effectively

3. RECORDS RELATING TO COINPORT'S AML/CTF PROGRAM

3.1 The AML/CTF Compliance Officer ("AML/CTF CO") ensures that the following records are retained:

- (a) this Program and each variation to it;
- (b) the Board of Directors' approval of this Program, and each variation to this Program;
- (c) AUSTRAC's feedback and correspondence;
- (d) external and internal AML/CTF reviews; and
- (e) correspondence with external lawyers on AML/CTF issues.

3.2 The records referred to in Section 3.1 are retained:

- (a) in the case of records relating to the adoption of each variation to this Program, during the period it or any part of it remains in force and for seven (7) years after it ceases to be in force; and
- (b) for the period of time determined by the AML/CTF Compliance Officer for all other records.

4. AUSTRAC ENROLMENT AND REGISTRATION

4.1 CoinPort is enrolled and registered with AUSTRAC as a Virtual Asset Service Provider (VASP). Prior to 31 March 2026, this registration was known as Digital Currency Exchange (DCE) registration.

CoinPort's AUSTRAC Details:

- Registered Digital Currency Exchange Number: 100633359
- Registered Independent Remittance Dealer Number: IND100633359-001
- Registration Date: 03 February 2020
- AUSTRAC Account Number (AAN): 100633359
- Legal Name: CoinPort PTY LTD

4.2 Virtual Asset Service Providers are required to enrol and register with AUSTRAC. Enrolling and registering are separate legal requirements and both must be completed. From 31 March 2026, AUSTRAC maintains a public VASP Register.

ENROLLING WITH AUSTRAC

Responsible Person	AML/CTF CO
Timeframe	CoinPort must enrol within twenty-eight (28) days of providing or commencing to provide a designated service.
Changes to Enrolment	Enrolment details must be kept up to date and AUSTRAC must be notified within fourteen (14) days of any changes to CoinPort's details. For further information refer to Section 28.

REGISTERING WITH AUSTRAC

Responsible Person	AML/CTF CO
Timeframe	Prior to providing or commencing to provide a designated service. A Registrable Virtual Asset Service must not be provided if CoinPort has not registered with AUSTRAC. Failure to register may constitute the commission of a criminal offence.
Registration Renewal	VASP registration must be renewed every three (3) years.

| Changes to Registration | Registration details must be kept up to date and AUSTRAC must be notified within fourteen (14) days of any changes to CoinPort's details. For further information refer to Section 28. |

5. PENALTIES

5.1 Failure to comply with the obligations u

nder the AML/CTF Act may result in civil or criminal penalties.

5.2 Civil penalties for contravention of the AML/CTF Act range up to $3.4 million for an individual and up to $17 million for a corporation.

5.3 The penalties for criminal offences include imprisonment for up to ten (10) years and/or fines up to $1.7 million.

6. REPORTING GROUPS (FORMERLY DESIGNATED BUSINESS GROUPS)

6.1 CoinPort is a reporting entity which does not currently share obligations with another person for the purposes of forming a Reporting Group under the AML/CTF Act and Rules. CoinPort does not intend to form and/or join an existing Reporting Group.

6.2 Note:

From 31 March 2026, the previous "Designated Business Group (DBG)" concept is replaced with a "Reporting Group" model. Each Reporting Group must appoint a "Lead Entity" responsible for overseeing group-wide compliance and risk management.

6.3 Another entity can join with CoinPort to form CoinPort's Reporting Group if:

- (a) that entity is:
    - (i) related to each other member of CoinPort's DBG within the meaning of section 50 of the Corporations Act 2001;
    - (ii) either:
        - (A) a reporting entity;
        - (B) a company in a foreign country which if it were resident in Australia would be a reporting entity; or
        - (c) providing a designated service pursuant to a joint venture agreement, to which each member of CoinPort's DBG is a party; and
    - (iii) not a member of another DBG; or
- (b) otherwise permitted by the AML/CTF Act or Rules.

6.4 When any changes in CoinPort's Reporting Group occur, the AML/CTF CO must notify AUSTRAC's CEO within fourteen (14) business days from the date the change takes effect.

7. DEFINITIONS

7.1 Words and phrases defined in the AML/CTF Act or Rules have the same meaning when used in this Program unless otherwise specified.

KEY DEFINITIONS

Australian Government Entity: The Commonwealth, a State or a Territory; or an agency or authority of the Commonwealth, State, or local governing body.

Authorised Officer: In accordance with section 5 of the AML/CTF Act, an authorised officer is the AUSTRAC CEO or a person for whom an appointment as an authorised officer is in force under section 145.

Beneficial Owner:

- (a) of a person who is a customer of a reporting entity, means an individual who ultimately owns or controls (directly or indirectly) the customer;
- (b) in this definition, control includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices;
- (c) in this definition, owns means ownership (either directly or indirectly) of 25% or more of a person.

Digital Currency: A digital representation of value that:

- (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
- (ii) is not issued by or under the authority of a government body; and
- (iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and

- (iv) is generally available to members of the public without any restriction on its use as consideration; or
- but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency.

Note:

From 31 March 2026, this definition is replaced with the broader "Virtual Asset" definition under the 2024 AML/CTF Amendment Act.

Virtual Asset: A digital representation of value that:

- (a) can be traded or transferred digitally; and
- (b) can be used for payment or investment purposes;
- but does not include digital representations of fiat currencies.

Virtual assets include cryptocurrencies, stablecoins, governance tokens, utility tokens, and certain NFTs that function as a medium of exchange.

Virtual Asset Service Provider (VASP): A person running a business that provides virtual asset services, including:

- (a) exchange between virtual assets and fiat currencies;
- (b) exchange between one or more forms of virtual assets;
- (c) transfer of virtual assets;
- (d) safekeeping or administration of virtual assets or instruments enabling control over virtual assets; or
- (e) participation in and provision of financial services related to virtual assets.

From 31 March 2026, this replaces the previous "Digital Currency Exchange Provider" terminology.

Digital Currency Exchange Provider (DCE): [Historical - replaced by VASP from 31 March 2026] A person running a business that exchanges digital currency with money or vice versa.

Politically Exposed Persons ("PEP"): An individual who holds a prominent public position or function in a government body or an international organisation, including their immediate family members and close associates.

Primary Photographic Identification Document: A passport, driver's licence, or national identity card containing a photograph of the person.

Primary Non-Photographic Identification Document: A birth certificate, citizenship certificate, or concession card.

Secondary Identification Document: A utility bill, government notice, or school notice issued within specified timeframes.

Reasonable Measures: Appropriate measures which are commensurate with the money laundering or terrorism financing risks.

Registrable Digital Currency Exchange Service: A designated service covered by item 50A of table 1 in section 6 of the AML/CTF Act.

Travel Rule: The requirement (effective March 2026) to collect, verify, and transmit originator and beneficiary information for all cryptocurrency transfers between VASPs, regardless of

transaction value. For transfers to/from self-hosted wallets, a threshold of AUD $10,000 applies.

VASP: Virtual Asset Service Provider - an entity providing virtual asset services including exchange, transfer, custody, or administration of virtual assets. From 31 March 2026, this replaces the previous "Digital Currency Exchange (DCE)" terminology in Australia, aligning with international FATF standards.

IVTS: International Value Transfer Service - replaces the previous term "International Funds Transfer Instruction (IFTI)" under the 2026 reforms. Includes instructions for transfers of value (money, property, or virtual assets) to or from foreign countries.

8. PURPOSE AND APPLICATION OF THIS PROGRAM

8.1 This Program is designed to identify, mitigate and manage the money laundering, terrorism financing, and proliferation financing (ML/TF/PF) risk which CoinPort may reasonably face in the provision of designated services. This Program adopts the outcomes-focused, risk-based approach mandated by the 2026 AML/CTF reforms (refer to Section 2A).

8.2 This Program applies to all aspects of CoinPort's business, to which the AML/CTF Act and the Rules are applicable and to any functions which are outsourced to third parties.

8.3 All CoinPort staff are given a copy of this Program and provided with necessary training so they understand the nature and purpose of CoinPort's business relationship with customers and CoinPort's obligations under the AML/CTF Act and Rules.

GOVERNANCE AND OVERSIGHT

9. OVERSIGHT BY THE BOARD OF DIRECTORS AND BOARD APPROVAL

9.1 This Program was approved and adopted by CoinPort's Board of Directors ("Board") on 5 January 2026.

9.2 Management Accountability (2026 Requirement):

CoinPort's Board and senior management must take "reasonable steps" to ensure CoinPort complies with this Program. This includes:

- Regular review of compliance metrics and risk indicators
- Timely response to identified deficiencies or adverse events
- Adequate resourcing of compliance functions (budget, personnel, technology)
- Setting appropriate "tone from the top" regarding compliance culture
- Ensuring the AML/CTF Compliance Officer has appropriate authority and independence

9.3 This Program is subject to ongoing oversight by the Board, senior management and CoinPort's AML/CTF CO, and:

- (a) The AML/CTF CO, in consultation with senior management, reviews this Program on at least an annual basis to ensure it is:

    - (i) drafted in accordance with the AML/CTF Act and Rules;
    - (ii) applicable and relevant to the functions of CoinPort's business operations; and
    - (iii) reflects any changes to CoinPort's designated services.
- (b) The review is presented to the Board at the next Board meeting; and
- (c) Any changes to this Program are required to be reviewed and approved by the Board.

9.4 Monthly meetings with the Board and senior management are held by the AML/CTF CO to report on:

- (a) significant changes to the ML or TF risks affecting CoinPort;
- (b) compliance with this Program, the AML/CTF Act and Rules by CoinPort;
- (c) the results of any internal or external review of this Program;
- (d) assessment of the ML and TF risks associated with any new product, delivery channels, business partners and operations;
- (e) any AUSTRAC feedback;
- (f) changes to relevant legislation; and
- (g) ongoing fraud detection and prevention to protect members of the exchange.

10. COINPORT'S AML/CTF COMPLIANCE OFFICER

10.1 CoinPort has appointed Nicanor Nuqui as CoinPort's AML/CTF CO for the purposes of the AML/CTF Act and Rules, and also the Nominated Contact Officer.

10.2 The AML/CTF CO reports to the Board of Directors and possesses sufficient skills and experience to carry out the roles of the AML/CTF CO.

10.3 The AML/CTF CO is responsible for implementing and over-seeing CoinPort's obligations under the AML/CTF Act and Rules, including but not limited to:

- (a) providing regulatory and legal updates in relation to the AML/CTF Act and Rules;
- (b) ongoing monitoring of the implementation of the Program;
- (c) considering and incorporating feedback from employees, clients and AUSTRAC;
- (d) ensuring overall compliance with the AML/CTF Act and Rules;
- (e) investigating suspicious matters, issues or incidents which may give rise to ML/TF risks;
- (f) maintaining records;
- (g) conducting employee risk awareness training;
- (h) ensuring appropriate fraud detection and prevention policies are implemented;
- (i) implementing and maintaining Travel Rule compliance systems (from March 2026); and
- (j) maintaining financial sanctions screening procedures.

10.4 The AML/CTF CO is authorised to act independently and to delegate responsibilities under this Program to another CoinPort employee, agent or responsible third party where reasonable to do so.

10.5 If CoinPort or any employee receives correspondence from AUSTRAC, those enquiries should be directed to the AML/CTF CO at first instance.

11. REVIEW OF THE PROGRAM

11.1 Internal Reviews

| Responsible Person | AML/CTF CO |
| Frequency | Quarterly (unless otherwise indicated based on factors below) |

When an internal review must be conducted:

- (a) Where a significant change in the ML/TF/PF risk relating to designated services has been identified;
- (b) prior to CoinPort introducing a new designated service to the market;
- (c) prior to CoinPort adopting a new method of delivering a designated service;
- (d) prior to CoinPort adopting new technology used for the provision of designated services;
- (e) where the AML/CTF CO identifies changes in the nature of business relationship, control structure or beneficial ownership of customers;
- (f) following any "adverse event" including:

    - Regulatory enforcement action or warning from AUSTRAC
    - Significant compliance breach or failure
    - Fraud incident affecting customers or CoinPort
    - Sanctions violation or near-miss
    - Travel Rule failure or systematic issue
    - Employee misconduct related to AML/CTF
    - Significant changes in sanctions lists affecting CoinPort's customers or operations
    - Identification of new ML/TF/PF typologies relevant to CoinPort's business;
- (g) when material changes occur in the business environment such as:
    - Entry into new markets or jurisdictions
    - Significant increase in transaction volumes (>50% increase)
    - Changes in customer demographics or risk profile
    - Introduction of new payment methods or blockchain networks
    - Adverse media coverage affecting CoinPort or the virtual asset sector
    - Regulatory guidance updates from AUSTRAC or FATF.

11.2 Independent Reviews

| Responsible Person | AML/CTF CO - report results to the Board |
| Frequency | Annually (with initial review 1 month post-implementation for major program changes) |

Special Note - 2026 Program Implementation:
Given the significant changes in Version 3.0 (unified program

structure, Travel Rule implementation, expanded customer types, new technology integration), CoinPort will conduct an initial independent review in February 2026 (one month after implementation) to identify any early issues or required adjustments. Following this initial review, annual reviews will occur each January thereafter.

Who should conduct the external review?

The independent party conducting the review must be independent and:

- (a) have not been involved in undertaking any functions required under this Program;
- (b) have not been involved in the design, development, implementation, maintenance or management of this Program;
- (c) have not been involved in the development of CoinPort's risk assessment or internal controls;
- (d) have access to employees and can make enquiries of any employee;
- (e) have access to records, personnel and property within privacy obligations;
- (f) be impartial and objective; and
- (g) be appropriately qualified to conduct the review.

What should be covered in the review?

The independent party must:

- (a) assess the effectiveness of this Program having regard to ML and TF risk;

- (b) assess whether this Program complies with the Rules;
- (c) assess whether this Program has been effectively implemented; and
- (d) assess whether CoinPort has complied with this Program.

The independent party may also:

- (a) assess risk management resources available including funding and staff allocation;
- (b) identify future needs relevant to the nature, size and complexity of CoinPort;
- (c) assess ongoing risk management procedures and controls;
- (d) assess Travel Rule implementation and effectiveness (from March 2026);
- (e) assess financial sanctions screening procedures and effectiveness.

12. AUSTRAC FEEDBACK

12.1 Where AUSTRAC provides CoinPort with feedback regarding performance in the management of ML/TF risk, any receipt of such feedback is immediately referred to the AML/CTF CO.

12.2 The AML/CTF CO assesses AUSTRAC's feedback to determine if any changes to this Program are required and implements changes as soon as reasonably practicable with the Board's approval.

MONEY LAUNDERING AND TERRORISM FINANCING

13. WHAT IS MONEY LAUNDERING?

13.1 Money laundering ("ML") is the process used to disguise the illegal origin of the proceeds of illegal activities such as drugs trafficking, tax evasion, smuggling, theft, terrorism, arms trafficking and corrupt practices.

13.2 There are three main stages of ML:

- (a) Placement – the physical disposal of the proceeds e.g. deposit into an account;
- (b) Layering – creating complex layers of financial transactions to separate the proceeds from their source and hide any audit trail;
- (c) Integration – taking the proceeds of ML and placing them back into the financial system so they appear legitimate.

14. WHAT IS TERRORISM FINANCING?

14.1 Terrorism financing ("TF") is often the reverse of ML whereby funds within a legitimate source are put into the financial system and redirected into the hands of terrorist organisations.

14.2 Terrorist organisations obtain money from:

- (a) Illegal Activities – drug trafficking, smuggling, kidnapping and extortion;
- (b) Rich Individuals;
- (c) Charitable and Religious Institutions;
- (d) Commercial Enterprises; and
- (e) State Sponsors.

14A. WHAT IS PROLIFERATION FINANCING?

14A.1 Proliferation financing ("PF") is 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.

14A.2 In simpler terms, PF is financing weapons of mass destruction (WMD) programs, including the networks and entities that support them.

14A.3 Proliferation financing activities may involve:

- (a) Front companies and shell corporations used to obscure the true purpose of transactions;
- (b) Trade in dual-use goods (items with both civilian and military applications) such as certain chemicals, metals, or technology components;

- (c) Financial transactions with entities in jurisdictions of proliferation concern (particularly North Korea and Iran);
- (d) Complex corporate structures designed to evade sanctions targeting WMD programs;
- (e) Use of financial systems to move funds for procurement of WMD-related materials;
- (f) Sanctions evasion techniques to access the international financial system despite targeted restrictions.

14A.4 Key differences between ML/TF and PF:

- Money Laundering (ML): Disguising illegal funds to make them appear legitimate
- Terrorism Financing (TF): Moving funds (legal or illegal) to terrorist organizations
- Proliferation Financing (PF): Moving funds or providing financial services to support WMD programs, often involving state actors and complex international trade networks

14A.5 PF was added as a mandatory risk consideration under the 2026 AML/CTF reforms, requiring CoinPort to:

- (a) Identify and assess PF risks specific to our business;
- (b) Screen against proliferation-related sanctions lists (UN, DFAT, OFAC);
- (c) Monitor for PF red flags including complex corporate structures that could be used for sanctions evasion;
- (d) Report suspicious matters that may relate to PF activities.

14A.6 CoinPort's PF risk profile is assessed as LOW-MEDIUM. See Appendix 3 Section 5 for detailed PF risk assessment and Section 26.2 for PF-specific sanctions controls.

15. DESIGNATED SERVICES PROVIDED BY COINPORT

15.1 CoinPort provides the following designated services:

- (a) Item 50 of section 6 of the AML/CTF Act; and
- (b) Item 50A of section 6 of the AML/CTF Act.

15.2 CoinPort deals in the following digital currencies:

- (a) Bitcoin (BTC) and various Bitcoin forks;
- (b) Ether (ETH) and various Ethereum blockchain tokens;
- (c) Ethereum Classic (ETC) and various tokens on other Ethereum blockchain forks;
- (d) Various tokens on the Tron blockchain;
- (e) Various tokens on the Ripple blockchain;
- (f) Various tokens on the Solana blockchain.

15.3 CoinPort undertakes due diligence on the supply sources of purchased digital currencies to ensure they are trusted and reliable. CoinPort will ensure it has a contractual agreement in place with digital currency supply sources prior to providing designated services.

15.4 CoinPort offers the following services to customers:

- (a) Buying digital currency;
- (b) Selling digital currency;
- (c) Exchanging digital currency;
- (d) Holding digital currency (on trust or as custodian).

15.5 CoinPort has undertaken assessment of ML/TF risks associated with its designated services taking into account:

- (a) nature, size and complexity of its business;
- (b) type of ML/TF risk that CoinPort might reasonably face;
- (c) customer types, including any politically exposed persons;
- (d) types of designated services provided;
- (e) methods by which services are delivered;
- (f) jurisdictions in which services are delivered;
- (g) responsible third parties to whom CoinPort outsources AML/CTF obligations;
- (h) any significant changes in ML/TF risk;
- (i) any ML/TF risk posed by new designated services, new delivery methods, or new technologies.

15.6 Significant Changes to Customer's Business:

If CoinPort notices significant changes to a customer's business, CoinPort obtains further details in writing to satisfy itself that the customer does not present an unacceptable risk. Significant changes include:

- (a) changes in the nature of the customer's business or business relationship;
- (b) changes in the customer's control structure;
- (c) changes in the customer's beneficial ownership; or
- (d) changes in the way a customer conducts transactions.

15.7 New Designated Services:

Prior to introducing a new service, the AML/CTF CO assesses whether it involves provision of a designated service and the ML/TF risk involved. Board approval must be received before introducing a new designated service.

RISK MANAGEMENT

16. RISK ASSESSMENT AND MANAGEMENT MATRIX

16.1 CoinPort has put in place a Risk Assessment and Management Matrix ("AML/CTF Matrix") which outlines assessment of various ML/TF/PF risks associated with designated services and the measures in place to control such risks. The AML/CTF Risk Matrix is attached at Appendix 3.

| Responsible Person | AML/CTF CO - review and update the AML/CTF Matrix regularly |

Risk identification of main ML/TF/PF risks:

- (a) Customer types
- (b) Products & services
- (c) Business practices & delivery methods
- (d) Countries we deal with
- (e) Proliferation financing risks (sanctions evasion, dual-use goods, WMD-related entities)

Risk Assessment/Measurement:

- (a) Likelihood – chance of risk happening
- (b) Impact – amount of loss or damage if risk occurs
- (c) Likelihood x impact – level of risk or risk score

Mitigating and managing risk:

- (a) Minimise and manage risks
- (b) Application of strategies, policies and procedures
- (c) Existing systems and controls
- (d) Risk plan including PF-specific sanctions screening

Risk Monitoring and Review:

- (a) Development and implementation of monitoring process
- (b) Record keeping
- (c) Review of risk plan and this Program following adverse events
- (d) Independent review

17. EMPLOYEE DUE DILIGENCE PROGRAM

17.1 CoinPort does not have any existing employees who are currently in a position to facilitate the commission of a ML/TF offence due to the requirement for at least two (2) account signatories to authorise any funds transfers.

17.2 New Employees

(a) The AML/CTF CO must be informed of all prospective new employees before they are issued with an employment contract. The prospective employee will be informed that their employment is subject to background checks.

(b) The AML/CTF CO must undertake a risk assessment for all newly created roles or previously existing roles to determine whether they will be in a position to facilitate the commission of a ML/TF offence.

(c) For all new employees, CoinPort must carry out the following checks prior to an offer of employment:

- (i) collect and verify their identification documents as if they are a new client;
- (ii) obtain a copy of their working visa (where the employee is not an Australian citizen);
- (iii) carry out at least two (2) reference checks;
- (iv) obtain copies of all tertiary educational qualifications or highest educational qualification;
- (v) carry out a criminal history check with the Australian Federal Police ("AFP"); and
- (vi) carry out a bankruptcy/credit check.

(d) If CoinPort determines the results to any of these procedures are not satisfactory, CoinPort will not offer that person employment.

17.3 Existing Employees

(a) Where CoinPort proposes to transfer or promote an existing employee to a new role, a risk assessment must be undertaken.

(b) Where an employee is transferred or promoted to a role that may put them in a position to facilitate the commission of a ML/TF offence, the AML/CTF CO will:

- (i) obtain an updated copy of the employee's working visa (where applicable); and
- (ii) carry out any other identification, reference, criminal history checks, bankruptcy or credit checks deemed necessary.

(c) Employees who fail to comply with procedures above will be reported to CoinPort's Board. Appropriate disciplinary action, including termination, will occur where necessary.

17.4 Copies of employee checks undertaken must be kept in accordance with CoinPort's Document Retention Policy.

17.5 Managing Non-Compliance

(a) CoinPort will, on an ongoing basis, monitor compliance with this Program.

(b) If an employee fails to comply with this Program, the matter will be referred to the AML/CTF CO immediately. The AML/CTF CO may then take any of the following actions:

- (i) undertake an internal spot check on the employee's performance;

- (ii) implement a higher level of supervision of the employee;
- (iii) provide a warning to the employee for non-compliance; or
- (iv) if breaches are repeated without reasonable excuse, consider transferring or dismissing the employee in consultation with the Board.

18. RISK AWARENESS TRAINING PROGRAM

18.1 CoinPort implements a Risk Awareness Training Program ("RATP") designed to ensure each employee receives appropriate ongoing training on the ML/TF/PF risk that CoinPort may face.

18.2 The RATP is designed to enable employees to understand:

- (a) CoinPort's obligations under the AML/CTF Act and Rules;
- (b) the consequences of non-compliance with the AML/CTF Act and Rules;
- (c) the type of ML/TF/PF risk that CoinPort might face and potential consequences;
- (d) what money laundering, terrorism financing, and proliferation financing are (Sections 13, 14, 14A);
- (e) processes and procedures provided for by this Program which are relevant to the employee's work;
- (f) Travel Rule requirements and procedures (from March 2026);
- (g) financial sanctions screening requirements including proliferation financing sanctions;

- (h) how to identify and report suspicious activities or red flag indicators;
- (i) the 2026 reforms and CoinPort's risk-based approach to compliance; and
- (j) tipping-off laws and when information sharing is permitted.

18.3 All new employees are required to undergo the RATP as part of their induction process. All employees in positions identified as having ML/TF risk are required to undertake training on an annual basis, or whenever the AML/CTF CO considers necessary.

18.4 The AML/CTF CO is responsible for maintaining the training register for both induction training and ongoing training conducted for each employee.

18.5 Ongoing Compliance Training – The AML/CTF CO may decide when compliance training by an external compliance consultant is necessary. The AML/CTF CO must, upon completion of training, make the training materials available to all employees.

18.6 In-house AML/CTF Seminars – The AML/CTF CO may organise in-house AML/CTF seminars on a regular basis so that employees returning from leave have the opportunity to refresh their knowledge.

18.7 Non-attendance of Training Sessions – Non-attendance at any training sessions, without reasonable excuse, will be reported to the Board and the AML/CTF CO will take any disciplinary action they consider necessary.

18.8 Compliance Policies – All new employees will receive a copy of this Program and all compliance policies within a reasonable time of commencing employment. All employees are expected to review these compliance policies regularly and complete a declaration stating that they have read the policies.

18.9 Document Retention Policy – The AML/CTF CO must encourage all employees to read and understand the Document Retention Policy.

19. OUTSOURCING

Prior to Outsourcing

Prior to CoinPort outsourcing any of its AML/CTF obligations, it will:

- (a) have an agreement in place with the party to whom the activities are outsourced ("Third Party Providers");
- (b) where relevant, require Third-Party Providers to implement the policies and procedures outlined in this Program;
- (c) assess the ML/TF risk associated with outsourcing the particular activity;
- (d) conduct due diligence on the activities outsourced to ensure that outsourcing will not increase the ML/TF risk;
- (e) conduct due diligence on Third-Party Providers to ensure that outsourcing to these parties will not increase the ML/TF risk;
- (f) ensure that all Third-Party Providers understand:

- (i) CoinPort's obligations under the AML/CTF Act and Rules;
- (ii) the consequences of non-compliance with the AML/CTF Act and Rules;
- (iii) the type of ML/TF risk CoinPort might face and potential consequences; and
- (iv) processes and procedures provided for by this Program relevant to the work.

Additional Due Diligence for Customer Identification Functions

In addition to the due diligence requirements above, CoinPort will:

- (a) conduct due diligence on Third-Party Providers to ensure they hold appropriate licences and/or registrations with ASIC, AUSTRAC or any other relevant regulator;
- (b) ensure Third Party Providers have an AML/CTF Policy in place which complies with the Act and Rules; and
- (c) ensure the agreement permits access to the KYC records of CoinPort's clients.

Reviews

The AML/CTF CO will undertake quarterly reviews of all Third-Party Providers to assess whether the Third-Party Provider:

- (a) has performed their functions within the scope of the agreement;
- (b) maintains appropriate resources, licences and registrations;
- (c) has met their AML/CTF obligations; and

- (d) has caused an increase in the ML/TF risk CoinPort faces.

19.1 CoinPort maintains a separate Third-Party Providers register:

Service Provider	Service Outsourced	Date of Appointment	Frequency of Review	Date of Last Review	Outcome
KYC-AID	KYC/AML Platform	1 January 2023	Annual	January 2026	No issues detected
Sumsub	KYC/AML Platform & Travel Rule	January 2026	Annual	January 2026	No issues detected
Notabene	Travel Rule Solution	January 2026	Annual	January 2026	Implementation in progress
AMLBot	Blockchain Analytics & Sanctions Screening	January 2026	Annual	Scheduled January 2027	Implementation completed, first annual review forthcoming

OPERATIONAL REQUIREMENTS

20. RECORD KEEPING OBLIGATIONS

20.1 When a customer identification procedure is required to be undertaken, a record of the following must be made:

- (a) the procedures undertaken; and
- (b) information obtained in the course of carrying out the procedure.

20.2 A copy of these records will be retained for at least seven (7) years after CoinPort has ceased to provide designated services to the customer.

20.3 Records to be retained (whether in electronic or hard copy form) must be easily identifiable, easily located and easily retrievable, in order to:

- (a) provide the record to an AUSTRAC authorised officer within a reasonable period; and
- (b) demonstrate to the AUSTRAC authorised officer that CoinPort has complied with obligations under subsection 112(2) of the AML/CTF Act.

20.4 A copy of any other record made by CoinPort or received from a customer in relation to the provision of a designated service must be retained for seven (7) years after the record is made or received.

20.5 Details of record keeping and handling are set out in CoinPort's Document Retention Policy.

20.6 Travel Rule Records (from March 2026): CoinPort must maintain for seven (7) years:

- (a) all Travel Rule messages sent and received;
- (b) all originator and beneficiary information collected;
- (c) screening results for Travel Rule transactions;
- (d) VASP counterparty communications;
- (e) risk assessments for unhosted wallet transactions.

21. TRANSACTION MONITORING

21.1 CoinPort's transaction monitoring program consists of three steps:

- (a) Monitoring all customer transactions in accordance with CoinPort's policies, systems and procedures;
- (b) Identifying all suspicious transactions; and
- (c) Taking the appropriate action.

21.2 The AML/CTF CO will review the transaction monitoring system in consultation with the Board and CoinPort's external compliance consultant.

21.3 The AML/CTF CO has primary responsibility for transaction monitoring. All transaction reports will be reviewed by the Board on a weekly basis.

21.4 All CoinPort employees will receive training in transaction monitoring as part of the RATP.

21.5 As required by the AML/CTF Act, CoinPort will provide reports to AUSTRAC in an approved form containing required information:

Compliance Obligations	Compliance Requirements	Compliance Actions	Responsible Person	Frequency
Annual AUSTRAC Compliance Report	Submit annual compliance report	Complete report per AUSTRAC regulations by 31 March each year	AML/CTF CO	Annually
Changes to AUSTRAC enrolment	Notify AUSTRAC of any change in business details	Report changes within fourteen (14) days	AML/CTF CO	As required - within 14 days
Suspicious Matter Reporting (SMR)	Implement and monitor SMR procedures	Submit SMRs within three (3) business days or twenty-four (24) hours for TF	AML/CTF CO	As required
Threshold Transaction Reporting (TTR)	Implement and monitor TTR procedures	Report TTRs within ten (10) business days	AML/CTF CO	As required
International Value Transfer Service (IVTS)	Implement and monitor IVTS procedures	Report IVTS within ten (10) business days	AML/CTF CO	As required
Travel Rule Reports	Implement Travel Rule reporting	Report as required under 2026 Travel Rule	AML/CTF CO	As required from March 2026

21.6 CoinPort will use the following methods for electronic reporting via AUSTRAC Online at https://online.austrac.gov.au:

- (a) Data entry: Manual entry into AUSTRAC Online account;
- (b) Spreadsheets: Using specially-designed spreadsheet or Excel templates;

- (c) Extraction: Using file format specifications or XML schemas to extract from existing database.

22. SUSPICIOUS MATTER REPORTING

22.1 CoinPort adopts a 'Red Flag' policy which requires employees to complete a Red Flag Indicator Sheet (Appendix 2) for each new client and as a procedure to conduct ongoing transaction monitoring.

General Rules

CoinPort must submit a SMR to AUSTRAC if:

- (a) CoinPort commences to provide, or proposes to provide, a designated service to a person; or
- (b) a person requests CoinPort provides a designated service; or
- (c) a person makes an enquiry about whether CoinPort would be willing to provide a designated service;

and CoinPort forms a suspicion on reasonable grounds that:

- (a) a person (or their agent) is not the person they claim to be, or
- (b) information CoinPort has may be:
    - (i) relevant to the investigation or prosecution of a person for an offence against a law;
    - (ii) relevant to the investigation or prosecution of an evasion or attempted evasion of a taxation law;
    - (iii) relevant to a ML/TF offence;

    - (iv) of assistance in the enforcement of laws relating to proceeds of crime; or
- (c) providing a designated service may be:
    - (i) preparatory to committing an offence related to ML or TF, or
    - (ii) relevant to the investigation or prosecution of a person for an offence related to ML or TF.

Who is Covered?

Existing, new or potential customers, or an agent of an existing, new or potential customer.

When to Report?

CoinPort must report a matter to AUSTRAC if a reasonable person would conclude from all circumstances and information available that an SMR must be submitted.

CoinPort's employees and AML/CTF CO are NOT expected to know or establish:

- (a) the exact nature of any criminal offence the customer may be involved in, or
- (b) that particular funds or property have been acquired through illicit means.

Red Flag Policy

CoinPort adopts a 'Red Flag' policy which requires employees to complete the Red Flag Indicators Sheet (Appendix 2).

Red Flag Indicators: CoinPort develops a list of Red Flag Indicators (Appendix 2). This sheet is updated on an ongoing basis.

CoinPort requires Appendix 2 to be completed:

- (a) for each new client – before the provision of a designated service; and
- (b) for existing clients – on a half yearly basis or whenever the AML/CTF CO considers necessary.

Reporting Line

Existence of 1 Red Flag:

Employee → Immediate Supervisor → AML/CTF CO → AUSTRAC

The employee responsible should:

- (a) conduct enhanced due diligence procedures and refer to immediate supervisor – the employee must not discuss the matter with anyone else except supervisor or AML/CTF CO;
- (b) the supervisor will report to AML/CTF CO once results of enhanced due diligence are received; and
- (c) the AML/CTF CO will then make an assessment on whether an SMR is required.

Suspicion Relating to Identity of Customer

If the AML/CTF CO is notified of a suspicion relating to the identity of the customer, the AML/CTF CO must, within fourteen (14) days, do one of the following:

- (a) review all KYC information in respect of the customer;
- (b) re-verify, from a reliable and independent source, any KYC Information obtained;
- (c) verify, from a reliable and independent source, any previously unverified KYC Information.

If after reviewing enhanced due diligence information the AML/CTF CO is still not satisfied that the customer is who they claim to be, or is unable to collect additional information, then the AML/CTF CO must make a SMR to AUSTRAC.

Suspicion Relating to Existing Customer

If the AML/CTF CO forms a reasonable suspicion in respect of an existing customer, the AML/CTF CO must, within fourteen (14) days, carry out the applicable customer identification procedures.

Discussion or Communication About the SMR

Immediate Supervisor or AML/CTF CO: CoinPort's employees must ONLY discuss the matter with their immediate supervisor, or the AML/CTF CO when their supervisor is not available, unless otherwise authorised.

After forming an initial suspicion, the employee should use discretion when making further enquiries to minimise the risk of the customer realising an SMR has been submitted.

AUSTRAC CEO: Once CoinPort has fulfilled the obligation to provide relevant information about a suspicious matter to AUSTRAC CEO, CoinPort's employees must not disclose to

anyone other than AUSTRAC CEO or AUSTRAC staff that the information has been communicated.

Submitting an SMR

If CoinPort's AML/CTF CO receives notification of a suspicious matter, the AML/CTF CO must:

- (a) assess the information which led the employee to form a suspicion; and
- (b) determine whether a SMR should be lodged.

If the AML/CTF CO determines that a SMR must be lodged, CoinPort will:

- (a) keep all records of results of any enhanced customer due diligence conducted; and
- (b) report the suspicion to AUSTRAC CEO through submitting an SMR in an approved form:
    - (i) within twenty-four (24) hours after forming the suspicion, if the matter relates to TF; or
    - (ii) in all other cases, within three (3) business days after forming the suspicion;
- (c) consult with AUSTRAC and other relevant enforcement agencies to determine how best to deal with the customer, if required; and
- (d) continue to transact with the customer on the usual basis until further advised.

Can CoinPort Continue Providing Services?

The AML/CTF Act does not direct reporting entities to stop providing designated services to, or terminate a business relationship with, a customer, even if CoinPort has formed a suspicion about that particular customer.

The AML/CTF CO will, after submitting an SMR, make an assessment as to whether to continue transacting with the customer. If CoinPort decides to continue the business relationship:

- (a) CoinPort must not disclose to the customer that it has formed a suspicion and/or communicated the suspicion to AUSTRAC – this is "tipping off"; and
- (b) CoinPort must continue to comply with the AML/CTF Act in all future dealings, which may include submitting additional SMRs.

Tipping Off Provisions

CoinPort must NOT disclose to any person (other than AUSTRAC) that it formed a suspicion about a customer or that it submitted an SMR to AUSTRAC. Doing so would constitute 'tipping off', which is an offence prohibited by section 123 of AML/CTF Act.

Reporting Entities that submit SMRs also have additional obligations not to disclose any:

- (a) information that might reasonably lead a person to conclude that they formed a suspicion about a customer or communicated that suspicion to AUSTRAC; and

- (b) requests from AUSTRAC for further information about an SMR report.

AUSTRAC considers that simply asking a customer for additional information (for example, about their identity or the source of funds) would not constitute an unlawful disclosure or tipping off offence.

Permitted Information Sharing (2025 Harm-Based Test)

2025 Reform - Harm-Based Tipping Off Test:

Under the updated tipping-off provisions effective from 2025, CoinPort may share information in certain circumstances where it does not prejudice an investigation or pose a risk of harm. Specifically:

Within a Reporting Group:

- If CoinPort is part of a Reporting Group (see Section 6), information may be shared between group members for the purpose of managing ML/TF/PF risks
- Information sharing must be documented and have a legitimate risk management purpose
- Must not be shared with the customer or in circumstances where it could reasonably tip off the customer
- Group members bound by same tipping-off obligations

With Professional Advisors:

- Information may be shared with legal practitioners to obtain legal advice on AML/CTF obligations

- Information may be shared with external auditors conducting independent reviews of this Program
- Information may be shared with compliance consultants assisting with risk assessments

With Other Regulated Entities:

- Limited information sharing permitted where necessary to manage ML/TF/PF risks
- Must not result in customer being tipped off about SMR or investigation
- Applies the "harm-based test": sharing is permitted if it would not prejudice an investigation or enforcement action

Harm-Based Test Application:
Before sharing any SMR-related information, the AML/CTF CO must assess:

1. Is the sharing necessary for a legitimate compliance or risk management purpose?
2. Would the sharing reasonably be expected to prejudice an AUSTRAC investigation or enforcement action?
3. Could the sharing result in the customer becoming aware that an SMR was filed?
4. Is the recipient bound by similar confidentiality obligations?

If sharing would likely prejudice an investigation or tip off the customer, it must not occur.

Documentation Required:

- All instances of permitted information sharing must be documented
- Rationale for sharing and harm-based test assessment must be recorded
- Recipient of information must be identified
- Date and nature of information shared must be logged

There are exemptions under the AML/CTF Act for the tipping off provisions which includes when CoinPort communicates a suspicion to a legal practitioner to obtain legal advice.

23. TRANSACTION REPORTING - THRESHOLD TRANSACTION REPORTS

Definitions

Physical Currency: The coin or printed money of Australia or another country which is designated as legal tender.

Digital Currency: A digital representation of value that:

- (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
- (ii) is not issued by or under the authority of a government body; and
- (iii) is interchangeable with money and may be used as consideration for supply of goods or services; and
- (iv) is generally available to members of the public without restriction on its use as consideration.

23.1 Under the AML/CTF Act, if CoinPort provides a designated service to a customer which involves the transfer of 'physical currency' or 'digital currency' of AUD10,000 or more (or the foreign currency equivalent), CoinPort must submit a threshold transaction report ("TTR") to AUSTRAC.

23.2 All employees of CoinPort must notify their immediate supervisor of any transactions relating to 'physical currency' or 'digital currency' with a value of AUD10,000 or more (or the foreign currency equivalent) immediately.

23.3 The supervisor will then report to CoinPort's AML/CTF CO on a daily basis and the AML/CTF CO will submit a TTR to AUSTRAC CEO within ten (10) business days of the threshold transaction taking place.

23.4 The TTR must be in the approved form and sent in accordance with the requirements of the Rules.

What Should Be Included in a TTR?

General Requirements:

- (a) The date of the threshold transaction;
- (b) A description of the designated service provided;
- (c) The total amount of funds provided to or received from the customer; and
- (d) Details of the threshold transaction, including whether it involved physical currency or digital currency.

Additional Requirement - if the customer is an individual:

- (a) the customer's full name;

- (b) any other name used by the customer, if known;
- (c) any business name(s) under which the customer operates, if known;
- (d) the customer's date of birth;
- (e) the customer's full address (not being a post office box address);
- (f) the postal address of the customer if different from their full address;
- (g) the customer's telephone number, if known;
- (h) the ABN of the customer, if known; and
- (i) if the person conducting the threshold transaction is not the customer, the details for the person.

Additional Requirement – if the customer is a business:

- (a) The name of the customer and any business name(s);
- (b) A description of the legal form of the customer and any business structure, if known;
- (c) The full address of the customer's principle place of business;
- (d) The postal address if different;
- (e) The ACN, ARBN and/or ABN, if known;
- (f) The customer's telephone number, if known; and
- (g) The details of the person conducting the threshold transaction.

24. TRANSACTION REPORTING INTERNATIONAL VALUE TRANSFER SERVICE (IVTS)

24.1 Under the AML/CTF Act, if a Reporting Entity sends or receives an instruction to or from a foreign country for a

transfer of value (including money, property, or virtual assets), they must submit an International Value Transfer Service ("IVTS") report to AUSTRAC.

24.2 The IVTS report must be in the approved form and sent in accordance with the requirements of the AML Rules.

IVTS Reporting

Rules: Under the AML/CTF Act, if a Reporting Entity sends or receives an instruction to or from a foreign country for a transfer of value under a value transfer arrangement, they must submit an IVTS report to AUSTRAC. The reporting obligations for IVTS are set out in section 45 and 46 of the AML/CTF Act.

IVTS: An electronic value transfer instruction is an electronic instruction sent between an ordering institution and a beneficiary institution. An International value transfer instruction occurs when:

- the ordering institution accepts the instruction at or through a permanent establishment in Australia and the transferred value is made available to the payee at or through a permanent establishment of the beneficiary institution in a foreign country (an outgoing IVTS); or
- the ordering institution accepts the instructions at or through a permanent establishment in a foreign country and the value is transferred to a permanent establishment of the receiving institution in Australia (an incoming IVTS).

There are two (2) types of IVTS:

- (a) IVTS (outgoing): Instructions transmitted out of Australia.
- (b) IVTS (incoming): Instructions transmitted into Australia.

CoinPort's Process

(a) When an employee receives an IVTS from a customer, they must refer this instruction immediately to their supervisor;
(b) The supervisor will report to the AML/CTF CO on a daily basis on all IVTS; and
(c) The AML/CTF CO must submit an IVTS report in an approved form to AUSTRAC CEO within ten (10) business days of the transaction taking place.

Information Required for an IVTS (Outgoing)

Minimum Information Required:

- (a) CoinPort must complete all required elements of the relevant form or spreadsheet via AUSTRAC Online.
- (b) Complete payer information pursuant to section 16.2(1) of the Rules.
- (c) Complete tracing information pursuant to section 16.2(2) of the Rules.

Complete Payer Information:

- (a) The name of the payer;
- (b) One of the following:

    - (i) the payer's full business or residential address (not a post office box);
    - (ii) a unique identification number given to the payer by the Commonwealth or an authority (e.g.: ABN or ACN);
    - (iii) a unique identification number given to the payer by the government of a foreign country;
    - (iv) the identification number given to the payer by the ordering institution; or
    - (v) if the payer is an individual—the payer's date of birth, the country of birth and the town, city or locality of birth; and
- (c) If the money is, or is to be, transferred from a single account held by the payer with the ordering institution in Australia—the account number or a unique reference number for the transfer instruction.

Complete Tracing Information:

- (a) If the money is to be transferred from an account held by the payer with the ordering institution—the account number; or
- (b) In any case—a unique reference number for the transfer instruction.

Information Required for an IVTS (Incoming)

Minimum Information Required:

- (a) CoinPort must complete all required elements of the relevant form or spreadsheet via AUSTRAC Online.

- (b) Complete payer information pursuant to section 16.3(3)(a) of the Rules.
- (c) Complete tracing information pursuant to section 16.2(3)(b) of the Rules.

Complete Tracing Information:

- (a) If the money is to be transferred from an account held by the payer with the ordering institution—the account number; or
- (b) In any case—a unique reference number for the transfer instruction.

IVTS Reports – Information on Person Completing Form

A report under subsection 45(2) of the AML/CTF Act must contain the following details about the person completing the report:

- (a) Full name;
- (b) Job title or position;
- (c) Telephone number; and
- (d) Email address.

25. TRAVEL RULE COMPLIANCE (2026 REQUIREMENTS)

25.1 Travel Rule Overview

Effective 31 March 2026, CoinPort must collect, verify, and transmit originator and beneficiary information for all

cryptocurrency transfers between Virtual Asset Service Providers (VASPs), regardless of transaction value.

CRITICAL: Australia has NO minimum threshold for VASP-to-VASP transfers. The Travel Rule applies to all virtual asset transfers between VASPs.

25.2 Information Collection Requirements

CRITICAL DISTINCTION - The $10,000 Threshold:

The AUD $10,000 threshold applies to AUSTRAC reporting for self-hosted wallets, NOT to the Travel Rule data collection obligations. There are three distinct scenarios:

Scenario 1: VASP-to-VASP Transfers (Exchange to Exchange)

NO MINIMUM THRESHOLD - Travel Rule Applies to ALL Amounts

Originator Information (must collect and verify):

- Full legal name
- Account number or unique transaction identifier
- Physical address (residential or business)
- Date and place of birth OR customer ID number

Beneficiary Information (must collect):

- Full legal name or registered business name
- Account number or wallet address
- Physical address (if available)

This applies whether the transfer is $1 or $1,000,000 AUD.

Scenario 2: VASP-to-Self-Hosted Wallet (Exchange to Private Wallet)

Travel Rule Does NOT Apply (there is no other VASP to exchange information with)

However, CoinPort has TWO separate duties:

Duty 1: Internal Collection Duty (ALL Amounts - No Threshold)

- CoinPort must collect and verify originator and beneficiary information for its own records
- Applies to transfers of ANY amount (e.g., $50, $500, $5,000, $50,000)
- **Minimum information to collect:**
    - Originator: Customer's verified identity (already on file)
    - Beneficiary: Name and wallet address
    - Customer attestation of wallet ownership (encouraged)
    - AMLBot blockchain analytics screening of destination wallet

Duty 2: AUSTRAC Reporting Obligation (≥ AUD $10,000 Threshold)

(a) Unverified Self-Hosted Wallets: For any transfer ≥ AUD $10,000 to or from a self-hosted wallet where the controller's

identity has not been verified, CoinPort must submit a report to AUSTRAC within 10 business days.

(b) Reporting Mechanism: Until AUSTRAC's new IVTS/Self-Hosted reporting forms are technically released, these transactions will be reported via the existing IFTI-E/DRA framework (or TTR if cash-linked).

(c) Future Compliance: Upon the formal commencement of the dedicated Self-Hosted Wallet Reporting obligation (as set by Ministerial rules), CoinPort will transition to the specific report type and format mandated by AUSTRAC.

(d) **Enhanced Due Diligence Requirements for ≥ AUD $10,000:**

- Customer must demonstrate wallet ownership (signature verification, test transaction, or declaration)
- Document source of funds for large unhosted transfers
- Senior management review may be required for very large amounts

Below AUD $10,000:

- Collect information for internal records (Duty 1)
- Standard AMLBot screening
- NO separate AUSTRAC reporting obligation for the self-hosted nature (standard IVTS reporting still applies if international)

At or Above AUD $10,000:

- Collect information for internal records (Duty 1)
- Enhanced due diligence and wallet ownership verification

- AUSTRAC reporting with self-hosted wallet notation (Duty 2)
- Document risk assessment and approval decision

Scenario 3: Self-Hosted Wallet to VASP (Private Wallet to Exchange) - INCOMING

Same principles as Scenario 2:

For ALL incoming deposits from self-hosted wallets:

- AMLBot blockchain analytics screening of source wallet
- Verify available originator information from customer
- Request additional information from customer if needed
- Document source of funds

For incoming deposits ≥ AUD $10,000 from self-hosted wallets:

- Enhanced blockchain analytics screening
- Customer must explain source of cryptocurrency
- Senior management review if high-risk indicators present
- AUSTRAC reporting if international transfer (IVTS - Section 24)
- Process deposit only if risk acceptable

25.3 Travel Rule Exemptions

The following are exempt from Travel Rule data exchange (but NOT from internal collection or AUSTRAC reporting duties):

- Transfers between CoinPort customer accounts (internal transfers - same entity)

- Transfers to/from self-hosted wallets (no counterparty VASP to exchange data with)
    - Note: Self-hosted transfers still require internal data collection (all amounts) and AUSTRAC reporting (≥$10k)

NO exemption exists for VASP-to-VASP transfers based on amount. All VASP-to-VASP transfers require full Travel Rule compliance regardless of value.

25.4 Travel Rule Technology Implementation

Solution Providers:

- Primary: Sumsub (integrated KYC and Travel Rule solution)
- Secondary: Notabene (Travel Rule network connectivity)

Technical Requirements:

- VASP identification and verification via Travel Rule protocol
- Secure encrypted message exchange (TRP, TRUST, or equivalent protocol)
- Real-time information validation
- Screening against sanctions lists pre-transmission
- Audit trail of all Travel Rule messages
- Integration with blockchain analytics
- VASP directory access for counterparty verification
- Support for “first-share” protocols between VASPs

VASP Counterparty Due Diligence (Mandatory Requirement):

CRITICAL: Before transmitting Travel Rule information to another VASP, CoinPort must conduct counterparty due diligence to determine on reasonable grounds:

Verification Requirements:

1. **Confirm the counterparty is a legitimate VASP:**

- Check VASP registration status with relevant regulator (AUSTRAC, FinCEN, FCA, etc.)
- Verify the counterparty appears on recognized VASP directories (Notabene Network, TRISA Directory, etc.)
- Confirm the counterparty has an AML/CTF program meeting regulatory standards

2. **Assess the counterparty's compliance capability:**

- Can the counterparty securely receive and safeguard PII (personally identifiable information)?
- Does the counterparty have capability to comply with Travel Rule obligations?
- Is the counterparty's AML/CTF program robust enough to protect transmitted data?

3. **Sanctions screening of counterparty:**

- Screen counterparty VASP against sanctions lists
- Verify counterparty is not operating illegally or without proper registration
- Check for adverse media or regulatory actions against counterparty

Due Diligence Sources:

- VASP registries (AUSTRAC public VASP Register, FinCEN MSB Registry, etc.)
- VASP directory services (Notabene, TRISA, TRP directories)
- Blockchain analytics provider VASP databases
- Public regulatory announcements and enforcement actions
- Industry reputation databases

If Counterparty Due Diligence Fails:

- CoinPort must NOT proceed with the transfer if:
    - Counterparty cannot be verified as a legitimate VASP
    - Counterparty appears on sanctions lists
    - Counterparty operating illegally or without registration
    - Counterparty cannot demonstrate adequate data protection capabilities
- Transaction must be declined and customer notified (without tipping off about specific concerns)
- Document decision rationale and inform senior management
- Consider filing SMR if suspicious circumstances identified

Ongoing Monitoring:

- Maintain list of approved counterparty VASPs
- Regular review (quarterly minimum) of counterparty compliance status

- Monitor for regulatory actions or adverse media regarding counterparties
- Remove counterparties from approved list if concerns identified

25.5 Travel Rule Procedures

Outbound Transfer Process (All VASP-to-VASP Transfers):

1. Customer initiates withdrawal to another VASP (any amount)
2. System automatically triggers Travel Rule data collection
3. Customer provides all required originator and beneficiary information
4. VASP Counterparty Due Diligence:
    - System identifies receiving VASP from wallet address or customer input
    - Verify beneficiary VASP registration and compliance status
    - Check beneficiary VASP against sanctions lists
    - Confirm beneficiary VASP can securely receive and protect data
    - If due diligence fails, decline transaction and document rationale
5. Sanctions screening of beneficiary (customer)
6. Travel Rule message sent to beneficiary VASP via secure protocol
7. Await confirmation from receiving VASP (reasonable timeframe)
8. Process transaction upon confirmation

9. Document decision and retain Travel Rule message records

If Beneficiary VASP Non-Responsive:

- Document outreach attempts (minimum 3 attempts over 24 hours)
- Escalate to AML/CTF CO for risk assessment
- Consider transaction hold, cancellation, or processing based on risk factors
- Document decision rationale including counterparty due diligence findings
- If pattern of non-responsiveness, remove VASP from approved counterparty list

Outbound Transfer Process (Self-Hosted Wallet ≥ AUD $10,000):

1. Customer initiates withdrawal to self-hosted wallet ≥ AUD $10,000
2. System triggers enhanced due diligence requirements
3. Collect full originator and beneficiary information
4. Enhanced blockchain analytics screening
5. Customer must demonstrate wallet ownership
6. Senior management approval for high-value transactions
7. Document risk assessment and decision
8. Process transaction if approved

Inbound Transfer Process (All VASP-to-VASP Transfers):

1. Receive Travel Rule message from originating VASP
2. Validate message authenticity and completeness

3. Match beneficiary information with CoinPort customer records
4. Sanctions screening of originator information
5. Confirm acceptance to originating VASP
6. Process incoming deposit
7. Flag any discrepancies for investigation

Inbound Transfer Process (Self-Hosted Wallet ≥ AUD $10,000):

1. Receive cryptocurrency from self-hosted wallet ≥ AUD $10,000
2. Enhanced blockchain analytics screening
3. Verify available originator information
4. Request additional information from customer if needed
5. Document source of funds
6. Senior management review if high-risk indicators present
7. Process deposit if risk acceptable

25.6 Travel Rule Record Keeping

- Maintain Travel Rule message records for minimum 7 years
- Store all originator/beneficiary information securely
- Audit logs of all Travel Rule transactions
- Documentation of screening results and risk decisions
- Records of VASP counterparty communications

25.7 Travel Rule Failure Scenarios

Non-Responsive Beneficiary VASP:

- Document outreach attempts (minimum 3 attempts over 24 hours)
- Escalate to senior management
- Consider transaction hold or cancellation based on risk assessment
- Document decision rationale

Incomplete or Invalid Information:

- Request clarification from customer or counterparty
- Do not process transfer until information is complete and verified
- Document information deficiencies and resolution
- Report to AUSTRAC if suspicious circumstances identified

Sanctions Hit:

- Immediately halt transaction
- Escalate to AML/CTF Compliance Officer
- Assess whether suspicious matter reporting required
- Comply with sanctions obligations (blocking/freezing)
- Document all actions taken

26. FINANCIAL SANCTIONS COMPLIANCE

26.1 Sanctions Framework

2026 Requirement: CoinPort must develop and maintain AML/CTF policies that ensure compliance with targeted

financial sanctions, including asset freezing, when providing designated services.

CoinPort complies with:

- Australian sanctions (DFAT Consolidated List per Autonomous Sanctions Act 2011 and Charter of the United Nations Act 1945)
- UN Security Council sanctions including proliferation financing sanctions
- Proliferation financing sanctions related to weapons of mass destruction (WMD) programs
- Extended jurisdiction considerations

26.2 Proliferation Financing Sanctions

CoinPort specifically screens for and monitors:

- Entities and individuals designated for involvement in WMD proliferation programs
- Entities in high-risk proliferation financing jurisdictions (North Korea, Iran sanctions programs)
- Dual-use goods transactions that could support WMD programs
- Front companies and facilitators of proliferation networks
- Sanctions related to ballistic missile and nuclear programs

PF Risk Assessment: CoinPort's proliferation financing risk is assessed as LOW-MEDIUM due to:

- Diverse customer base including corporate entities and institutional clients (requires enhanced screening)

- Potential for corporate front companies (mitigated through beneficial ownership verification)
- No trade finance or international goods transactions (reduces risk)
- No business in jurisdictions of PF concern
- Comprehensive sanctions screening including PF-related designations
- Enhanced beneficial ownership verification for all corporate structures

26.3 Sanctions Screening Procedures

Customer-Level Screening:

- All customers screened at onboarding against sanctions lists (DFAT, UN, OFAC, EU, UK)
- Daily automated re-screening of entire customer database
- Manual review of potential matches (fuzzy matching)
- Escalation of confirmed matches to senior management

Transaction-Level Screening:

- All transactions screened in real-time before processing
- Blockchain addresses screened via AMLBot for:
    - Sanctioned wallet addresses (OFAC SDN, DFAT, UN lists)
    - Blacklisted cryptocurrency exchanges
    - High-risk counterparties (darknet markets, ransomware, theft)
    - Mixing services and tumblers

    - Wallets associated with sanctioned jurisdictions
- Manual review of medium/high-risk AMLBot alerts
- Escalation of confirmed sanctions hits to AML/CTF CO

26.4 Sanctions Hit Response

1. Immediate Hold: Stop transaction processing immediately
2. Verification: Confirm match is true positive (vs. false positive)
3. Asset Freeze: If confirmed match, freeze customer funds/assets
4. Reporting: Report to DFAT and AUSTRAC as required
5. Documentation: Maintain detailed records of actions taken
6. No Tipping-Off: Do not inform customer of sanctions status
7. Legal Consultation: Engage legal counsel for complex matters
8. Ongoing Monitoring: Monitor for attempted circumvention

26.5 Screening Databases

CoinPort screens against:

- DFAT Consolidated List (Australian sanctions)
- UN Security Council Consolidated List
- OFAC SDN List (US sanctions - where applicable)
- EU Sanctions List
- UK HM Treasury Sanctions

27. AML/CTF COMPLIANCE REPORTS

27.1 CoinPort is required to submit an AML/CTF Compliance Report to AUSTRAC between 3 January and 31 March for the preceding calendar year in the form specified by AUSTRAC.

27.2 The AML/CTF CO is responsible for the submission of this report.

28. CHANGES TO COINPORT'S AUSTRAC ENROLMENT DETAILS

28.1 Part 8.9.1 of the Rules outlines the requirement of CoinPort to report to AUSTRAC any material changes in circumstances under section 75M of the AML/CTF Act.

28.2 CoinPort is required to report the following changes in its enrolment and registration details to AUSTRAC within fourteen (14) days of the change:

- (a) changes to enrolment details on AUSTRAC Business Profile Form;
- (b) changes in the number of key personnel and a declaration that police and bankruptcy checks have been obtained;
- (c) whether any key personnel have been criminally charged;
- (d) whether CoinPort is the subject of civil or criminal proceedings or enforcement action; and
- (e) changes to VASP registration details, including services provided and business activities.

28.3 Notification of a change of CoinPort's enrolment or registration details may be made by an agent of CoinPort where there is a current written agreement in place authorising the agent to notify changes on behalf of CoinPort.

29. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

29.1 Where CoinPort has provided or is providing a designated service to a customer and the AML/CTF CO believes, on reasonable grounds, that a customer has information that may assist CoinPort in the identification, management and mitigation of ML or TF risk, the AML/CTF CO may request the customer to provide such information. The request must be provided in writing and notify the customer that if the request is not complied with, then CoinPort may:

- (a) refuse to continue to provide a designated service;
- (b) refuse to commence to provide a designated service; or
- (c) restrict or limit the provision of the designated service.

29.2 If the customer does not comply with the request within a reasonable time then the AML/CTF CO may determine that, until the information is provided, CoinPort will take any of the actions in section 29.1(a) – (c).

29.3 In these circumstances, the AML/CTF CO will determine whether the matter should be reported to AUSTRAC as a suspicious matter (refer to section 22).

30. ONGOING CUSTOMER DUE DILIGENCE

30.1 CoinPort, as a Virtual Asset Service Provider (VASP), will monitor its customers for the purpose of identifying, mitigating and managing the ML/TF risk that the provision of a designated service may involve.

30.2 CoinPort will comply with the ongoing customer due diligence procedures outlined below.

Types of Customers

Customers CoinPort provides services to:

- (a) Individuals (including sole traders)
- (b) Companies (Australian domestic and foreign registered)
- (c) Trusts (regulated and unregulated)
- (d) Trustees and beneficiaries
- (e) Partnerships
- (f) Self-Managed Super Funds (SMSFs)
- (g) Institutional clients (superannuation funds, corporate treasury)
- (h) Associations (if applicable)
- (i) Registered cooperatives (if applicable)

Customers CoinPort will generally NOT provide services to:

- (a) Government bodies (unless specific risk assessment conducted)
- (b) Entities in sanctioned jurisdictions
- (c) Unlicensed money services businesses
- (d) Entities that cannot provide adequate KYC documentation

Review of Customer Types: The AML/CTF CO is responsible for reviewing and updating the customer types that CoinPort provides services to on an ongoing basis.

Monitoring Systems

CoinPort will monitor customers by implementing systems to:

- (a) collect further KYC Information for ongoing customer due diligence;
- (b) update and verify KYC Information;
- (c) monitor the transactions of customers; and
- (d) conduct enhanced customer due diligence in respect of high risk customers and customers about whom a suspicion has been formed.

Grouping of Customers

As part of implementing systems for ongoing customer due diligence, CoinPort will group customers according to their level of risk, assessed as part of the risk assessment procedures. The risk grouping will determine:

- (a) what further KYC Information needs to be collected;

- (b) what level of transaction monitoring needs to be conducted; and
- (c) whether enhanced customer due diligence program needs to be applied.

The AML/CTF CO is responsible for grouping of customers. The AML/CTF CO will review the grouping of customers on a monthly basis, and the Board will conduct spot check on the grouping of customers on a half-yearly basis.

Additional KYC Information

Risk Assessment for New Activities and Technologies: In undertaking risk assessment for new activities and technologies, the AML/CTF CO will determine whether any additional KYC Information or Beneficial Owner information should be collected from relevant customers either before any designated services are provided or during the course of CoinPort's relationship with the customer.

Assessment on Level of ML/TF Risk:

Based on the assessed level of ML/TF risk involved in provision of designated services, CoinPort has determined that:

- (i) Low Risk Customers - no additional KYC Information needs to be collected;
- (ii) Medium Risk Customers - the AML/CTF CO will determine what additional KYC Information or Beneficial Owner information will be collected;

- (iii) High Risk Customers - the AML/CTF CO will determine what additional KYC Information or Beneficial Owner information will be collected.

New Customers: In respect of a new customer, additional KYC Information will be collected at the same time as and in the same manner as KYC Information is required to be collected. Failure to provide additional KYC Information will be treated in the same way as failure to provide any other KYC Information.

Existing Customers: In respect of an existing customer or Beneficial Owner, CoinPort will update and re-verify KYC Information by requesting additional KYC Information where the AML/CTF CO considers the KYC Information is no longer up-to-date, incomplete or unreliable. CoinPort may also request additional KYC information where the scope of services provided to an existing customer changes.

When to Update and Re-verify KYC Information:

CoinPort will update and re-verify KYC Information in respect of a customer where:

- (a) the customer engages in a significant transaction or series of transactions, where a significant transaction occurs if a transaction or series of transactions conducted within any calendar month exceeds Ten Thousand Dollars ($10,000.00) of digital currency or physical currency in value; or
- (b) a significant change occurs:
    - (i) in the way the customer conducts transactions;

- (ii) in the nature of the customer's business or business relationship;
- (iii) in the customer's control structure;
- (iv) in the customer's beneficial ownership; or
- (v) in the number of transactions carried out by a customer increases by 100% within a five (5) calendar day period.

Where one of the above circumstances arises and the applicable customer identification procedure has not previously been carried out (i.e. the customer is a pre-commencement customer), CoinPort will carry out the applicable customer identification procedure and collect the relevant additional KYC Information.

Where a change in customer information relates to name, residential address, company registration number, trustee, name of trust, or identity of partner, CoinPort will seek to verify the updated KYC Information using reliable and independent documentation.

Transaction Monitoring Program

Responsible Persons: The Director and the AML/CTF CO have overall responsibility and oversight of CoinPort's transaction-monitoring program. CoinPort conducts transaction monitoring on a monthly basis.

Identification of Risk Factors: The AML/CTF CO must identify ML/TF risk factors relevant to customers of particular services and products. Such risk factors include:

- (a) value of the transaction exceeds Ten Thousand Dollars ($10,000.00) of digital currency or physical currency in value;
- (b) volume of transactions conducted by a customer within a five (5) calendar day period has increased by more than one hundred per cent (100%);
- (c) transaction involves foreign countries, customers or third parties against whom sanctions have been imposed or have been included on lists maintained by the Department of Foreign Affairs and Trade;
- (d) transaction involves a customer or third party who is a PEP;
- (e) AMLBot blockchain analytics indicate links to high-risk addresses, sanctioned wallets, blacklisted exchanges, or mixing services;
- (f) Travel Rule information incomplete or suspicious for any VASP-to-VASP transfer (from March 2026);
- (g) High-value transfers to/from self-hosted wallets (≥ AUD $10,000);
- (h) Non-compliance with Travel Rule requirements by counterparty VASPs;
- (i) AMLBot flags wallet addresses associated with darknet markets, ransomware, or theft;
- (j) Deposits from exchanges or wallets flagged as high-risk by AMLBot.

Steps After Risk Factors Identified:

- (a) An employee must immediately inform the AML/CTF CO when any ML or TF risk factor(s) are identified;

- (b) The AML/CTF CO will then liaise with the Board in relation to any further action;
- (c) Where an employee identifies a customer or third party of a kind specified above, the AML/CTF CO will take appropriate action to determine, with a reasonable degree of certainty, whether the customer or third party is that person.

Further Actions: If it is determined, as a result of transaction monitoring, that:

- (a) a customer should be placed in a higher risk grouping, CoinPort will collect additional KYC Information if required;
- (b) KYC Information needs to be updated or verified, CoinPort will update or verify the required information;
- (c) a customer is a high-risk customer, CoinPort will apply the enhanced customer due diligence program; or
- (d) a suspicious matter report needs to be lodged, CoinPort will follow the procedure outlined in Section 22.

Training on Identification of Risk Factors: In addition to the Risk Awareness Training, the AML/CTF CO will ensure that all employees who have direct contact with customers or their representatives receive regular training in the identification of ML/TF risk factors.

Review and Update: The AML/CTF CO, in consultation with the Board, must regularly assess CoinPort's transaction monitoring program and take steps to have this modified appropriately when required.

Enhanced Customer Due Diligence Program

Responsible Persons: The AML/CTF CO has overall responsibility and oversight of CoinPort's enhanced customer due diligence program.

Factors for Conducting Enhanced Customer Due Diligence:

The ML/TF risk associated with a particular designated service, customer, delivery method or jurisdiction is high, including but not limited to when:

- (a) the customer:
    - (i) is engaged in business which involves a significant number of cash transactions or amounts of cash; or
    - (ii) uses a complex business ownership structure for no apparent commercial reason; or
    - (iii) is based in, or conducts business through or in, a high-risk jurisdiction; or
    - (iv) cannot provide information to verify the source of funds; or
    - (v) requests an undue level of secrecy in relation to a designated service; or
    - (vi) is a PEP; or
- (b) a designated service is being provided to a customer who is or who has a Beneficial Owner who is, a foreign politically exposed person; or
- (c) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act (refer to Section 22); or

- (d) CoinPort is entering into or proposing to enter into a transaction and a party to the transaction is physically present, or is a company incorporated in, a prescribed foreign country; or
- (e) blockchain analytics indicate high-risk transaction patterns or wallet associations; or
- (f) Travel Rule information is incomplete, inconsistent, or indicates unusual cross-border transaction patterns (from March 2026); or
- (g) Large transfers to/from self-hosted wallets (≥ AUD $10,000) with insufficient explanation.

Steps After Factors Identified:

Where one or more of the factors above arises, the AML/CTF CO will arrange for one or more of the following due diligence procedures:

- (a) seek further information from the customer or from third party sources to:
    - (i) clarify or update the customer's KYC Information or Beneficial Owner information;
    - (ii) obtain any further KYC Information or Beneficial Owner information including taking reasonable measures to identify:
        - A. the source of the customer's and each Beneficial Owner's wealth; and
        - B. the source of the customer's and each Beneficial Owner's funds; and

    - (iii) clarify the nature of the customer's ongoing business with CoinPort.
- (b) conduct more detailed analysis in respect of the customer's KYC Information and Beneficial Owner information taking reasonable measures to identify the source of wealth and funds;
- (c) verify or re-verify KYC Information or Beneficial Owner information;
- (d) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future, including:
    - (i) the purpose, reasons for, or nature of specific transactions;
    - (ii) the expected nature and level of transaction behaviour, including future transactions;
- (e) consider whether a Suspicious Matter Report ought to be lodged;
- (f) seek senior manager approval for:
    - (i) continuing a business relationship with a customer; and
    - (ii) whether a designated service should continue to be provided; and
- (g) consider whether a transaction or particular transactions should be processed.

CUSTOMER IDENTIFICATION PROCEDURES

31. INTRODUCTION TO CUSTOMER IDENTIFICATION

31.1 This section sets out customer identification procedures for CoinPort's customers.

31.2 These procedures include:

- (a) prescribed processes for the collection and verification of KYC Information; and
- (b) risk based systems and controls to determine what (if any) other information will be collected and verified, having regard to money laundering or terrorism financing risk relevant to provision of CoinPort's designated services.

31.3 CoinPort will consider the following factors when identifying its risk exposure to money laundering or terrorism financing:

- (a) its customer types; including:
    - (i) Beneficial Owners of customers; and
    - (ii) any politically exposed persons;
- (b) customers' sources of funds and wealth;
- (c) nature and purpose of the business relationship with customers;
- (d) control structure of non-individual customers;
- (e) types of designated services provided;

- (f) methods by which designated services are delivered; and
- (g) foreign jurisdiction with which it deals.

31.4 Appendix 3 – Risk Assessment and Management Matrix details CoinPort's risk assessment procedures with respect to its customer types.

32. APPLICATION AND KYC CONSIDERATIONS

32.1 Customer identification and verification procedures must be carried out by CoinPort or a responsible third party:

- (a) prior to commencing to provide a designated service to a customer (other than an existing customer), unless CoinPort has already carried out the applicable customer identification procedure in respect of the customer; and
- (b) when CoinPort's employee is responsible for the customer (or another CoinPort employee on their behalf), unless the AML/CTF CO authorises that these procedures can be conducted by an external party.

32.2 The same KYC procedures will be applied across all CoinPort's customers to ensure that additional procedures do not need to be carried out where a customer uses more than one of CoinPort's designated services.

32.3 Where CoinPort outsources the customer identification and verification procedures to a responsible third party, the AML/CTF CO maintains overall responsibility for KYC obligations.

KYC Considerations

32.4 Once information relating to a customer has been collected and verified, CoinPort will re-assess the money laundering or terrorism financing risk posed by the customer.

32.5 In re-assessing the AML/CTF risk for each customer, CoinPort may consider, where appropriate and among other factors, whether:

- (a) the customer is unwilling to produce evidence of identification or produces unsatisfactory evidence;
- (b) the customer wishes to deal only in large amounts of cash and not in traceable bank transfers;
- (c) the customer or group of customers makes frequent transactions to the same individual or group;
- (d) the customer is willing to pay very high charges to complete a transaction;
- (e) the customer's normal remitting behaviour changes and they are unwilling to explain the reason or the source of the increase funds;
- (f) the customer is involved in a complex business ownership structure with no legitimate commercial rationale;
- (g) the non-individual customer has a complex business structure with little commercial justification, which obscures the identity of ultimate beneficiaries;
- (h) the customer is in a position which may expose CoinPort to the possibility of corruption;

- (i) the customer is based in, or conducting business through or in, a high-risk jurisdiction;
- (j) the customer is engaged in business which involves significant amounts of cash;
- (k) there is no clear commercial rationale for the customer seeking a designated service;
- (l) the customer is a PEP;
- (m) an undue level of secrecy is requested regarding a designated service;
- (n) the source of funds is difficult to verify;
- (o) the Beneficial Owners of a non-individual customer are difficult to identify and/or verify;
- (p) the Beneficial Owners of the non-individual customer are a resident in a high-risk jurisdiction;
- (q) there is a one-off transaction in comparison with an ongoing business relationship or series of transactions;
- (r) a designated service can be used for money laundering or terrorism financing;
- (s) the customer makes or accepts payments to or from accounts which have not been identified by CoinPort;
- (t) the customer makes or accepts payments to or from offshore accounts;
- (u) the customer has access to offshore funds;
- (v) the customer when migrating from one designated service to another carries a different type and level of AML/CTF risk;
- (w) the customer has income which is not employment-based or from a regular known source;
- (x) the customer is new, rather than having a long-term and active business relationship with CoinPort;

- (y) the customer's business is primarily of a money remittance service nature;
- (z) the customer's business is registered in a foreign jurisdiction with no local operations or domicile;
- (aa) the customer's business is an unregistered charity, foundation or cultural association;
- (bb) the customer is represented by another person, such as under a power of attorney.

Fraud Detection and Prevention

32.6 A major risk is that criminal fraudsters may attempt to use the exchange platform to disperse, launder and transfer funds from local members to places outside jurisdiction as blockchain transfers.

32.7 Exchange members vulnerable to fraud need to be identified and additional steps taken to protect them against fraud.

32.8 CoinPort has identified that certain categories of people are more susceptible to fraud. These people need to be identified and manual intervention performed to validate them as genuine cryptocurrency traders.

32.9 At the second step of the client on-boarding process, members are required to input their date of birth.

- (i) If the new member is more than 55 years of age a member of the support staff must phone and speak with them.

- (ii) Questions should be asked about their interest and knowledge of cryptocurrencies and blockchain technology.
- (iii) Details of these conversations must be logged in detail in the Fresh Desk support database.
- (iv) If the new member is identified as a potential fraud victim they should be advised of concerns.
- (v) Likely fraud victims must have their User status set to "banned" to prevent access to the exchange platform.

Risk Exposure Categories

32.10 CoinPort has made the following assessment in relation to risk categories of its customers:

Risk Exposure	Information to be collected	Certified Documents Required?
Low	Minimum information	No
Medium	Minimum + at least 1 piece of additional information	Yes. See List of Certifiers at Appendix 1.
High	Minimum + at least 2 pieces of additional information	Yes. See List of Certifiers at Appendix 1.

*This table applies to customer types as described in following sections, except where the AML/CTF Rules require CoinPort to collect certified documents.

33. RELIABLE AND INDEPENDENT ELECTRONIC DATA

33.1 Where CoinPort has determined that it will rely on reliable and independent electronic data in relation to verification of its customers, CoinPort must determine:

- (a) the accuracy of the data;
- (b) how secure the data is;
- (c) how the data is kept up-to-date;
- (d) how comprehensive the data is;
- (e) whether the data has been verified from a reliable and independent source;
- (f) whether the data is maintained by a government body or pursuant to legislation; and
- (g) whether the electronic data can be additionally authenticated.

34. INDIVIDUALS: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – CATEGORISATION OF CUSTOMERS

Where a new customer is an individual, CoinPort categorises the customer as one of the following:

1. Individual customer;
2. Customer with a joint account between a husband and wife with the same address;
3. Customer with a joint account with different surnames but with the same address;
4. Customer with a joint account with different addresses; or
5. Sole trader.

STEP 2 – IDENTIFICATION AND VERIFICATION

Customer Categories: 1-4 (Individual and Joint Accounts)

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect
Minimum	Minimum	1. Reliable and Independent Documentation
1. Full name	1. Name; and	Photographic:
2. Residential address; and	2. Residential address or Date of Birth	• Australian driver's licence containing photograph
3. Date of Birth		• Australian passport (may be expired within preceding 2 years)
		• Card issued under State/Territory law for proving age
		• Current foreign government issued passport or similar travel document
		• National Identity Card issued by foreign government
		• Foreign driver's licence
Additional	Additional	Non-Photographic:
1. customer's former name(s)	Any other additional information collected	• Australian Birth Certificate

2. occupation or business activities		• Australian Citizenship Certificate
3. source of funds including origin		• Birth Certificate issued by foreign government
4. income and assets		• Citizen Certificate issued by foreign government
5. nature and level of intended transaction behaviour		• Concession card as defined under Social Security Act 1991
6. beneficial ownership of funds		
7. details of employment		Where any document is in a language that is not English, it must be accompanied by an English translation prepared by an accredited translator.
		2. Reliable and Independent Electronic Data
		Electronic verification via KYC-AID or Sumsub platforms

Customer Category: 5 (Sole Traders)

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect

Minimum	Minimum	Same as above for individuals
1. customer's full name	1. Name; and	
2. customer's date of birth	2. Residential address or date of birth	
3. full business name (if any)		
4. full address of principal place of business (if any) or residential address		
5. ABN issued to the customer		
Additional	Additional	
Same as above for individuals	Any other additional information collected	

35. COMPANIES: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – CATEGORISATION OF CUSTOMERS

Where a new customer is a company, either domestic or foreign, CoinPort must be reasonably satisfied that the company exists and categorise the customer as one of the following:

1. an Australian domestic company;

2. an ASIC registered foreign company; or
3. an unregistered foreign company.

STEP 2 – IDENTIFICATION OF THE TYPES OF COMPANIES

Company Types:

Australian Domestic Company	Procedure
(a) listed public company	Apply Step 3(i) simplified verification procedure
(b) a majority owned subsidiary of an Australian listed public company	Apply Step 3(i) simplified verification procedure
(c) licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company	Apply Step 3(i) simplified verification procedure
(d) all other domestic companies	Apply Step 3(ii) verification procedure for all other domestic companies

ASIC Registered Foreign Company	Procedure
(a) majority owned subsidiary of an Australian listed public company	Apply Step 3(i) simplified verification procedure
(b) proprietary companies	Apply Step 3(iii) verification

	procedure for all other ASIC registered foreign companies
(c) unlisted public companies	Apply Step 3(iii) verification procedure for all other ASIC registered foreign companies
(d) listed public companies (from comparable jurisdictions)	Apply Step 3(i) simplified verification procedure

Unregistered Foreign Company	Procedure
(a) a majority owned subsidiary of an Australian listed public company	Apply Step 3(i) simplified verification procedure
(b) A foreign public company listed on an Australian comparable stock exchange	Apply Step 3(i) simplified verification procedure
(c) Proprietary and unlisted public foreign companies	Apply Step 3(iv) verification procedure for all other ASIC unregistered foreign companies
(d) A foreign public company not listed on an Australian comparable stock exchange	Apply Step 3(iv) verification procedure for all other ASIC unregistered foreign companies

Comparable Stock Exchanges – list of foreign or equivalent stock exchanges that are approved by ASIC for recognition, including but not limited to the following financial markets:

Country	Stock Exchange
Australia	Asia Pacific Exchange Limited, ASX Limited, Chi-X Australia Pty Ltd, National Stock Exchange of Australia Limited, SIM Venture Securities Exchange Ltd
Belgium	Euronext Brussels – Brussels Stock Exchange (BSE)
Canada	Toronto Stock Exchange (TSX)
Denmark	Copenhagen Stock Exchange (CSE)
Finland	Helsinki Stock Exchange (HEL)
France	Paris – SBF (PAR)
Germany	Frankfurt (FRA)
Hong Kong	Hong Kong Exchanged (HKEx)
Iceland	Iceland Stock Exchange (ICEX)
Ireland	Irish Stock Exchange (ISE)
Japan	Tokyo Stock Exchange (TSE)
Luxembourg	Luxembourg Stock Exchange (LUX)
Netherlands	Euronext Amsterdam
New Zealand	New Zealand Exchange (NZX)
Norway	Oslo Børs – Oslo Stock Exchange (OSE)
Singapore	Singapore Exchange (SGX)
Sweden	OMX Stockholm
Switzerland	Swiss Exchange (SWX)
United Kingdom	London Stock Exchange (LSE), Euronext - liffe
United States of America	New York Stock Exchange (NYSE), NASDAQ OMX, NASDAQ Stock Market

STEP 3 – IDENTIFICATION AND VERIFICATION PROCEDURES

(i) Simplified Verification Procedures

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
For an Australian Company - Minimum Information		
1. the full name of the company as registered by the Australian Securities and Investments Commission; 2. the full address of the company's registered office; 3. the full address of the company's principal place of business (if any); 4. the ACN issued to the company; 5. whether the company is registered by ASIC as a proprietary or public company; and 6. if the company is	1. Verify that the company is one of the following: • an Australian listed public company; • a majority owned subsidiary of an Australian listed public company; or • licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a	1. Verify the information collected by obtaining one or a combination of the following documents: • a search of the relevant Australian stock exchange; • a public document issued by the relevant company (for example, annual report); • a search of the relevant ASIC database; • a search of the license or other

registered as a proprietary company, the name of each Director of the company.	company.	records of the relevant Commonwealth, State or Territory regulator.
For an ASIC Registered Foreign Company - Minimum Information		
1. the full name of the company as registered by ASIC; 2. the full address of the company's registered office in Australia; 3. the full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia (if any); 4. the ARBN issued to the company; 5. the country in which the company was formed, incorporated or registered;		

6. whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and 7. if the company is registered as a private company by the relevant foreign registration body - the name of each Director of the company.		
For an Unregistered Foreign Company - Minimum Information		
1. the full name of the company; 2. the country in which the company was formed, incorporated or registered; 3. whether the	1. Verify that the company is one of the following: • an Australian listed public company; • a majority owned subsidiary	1. Verify the information collected by obtaining one or a combination of the following documents: • a search of the

company is registered by the relevant foreign registration body and if so: 4. any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration; 5. the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and 6. whether it is registered as a private or public company or some other type of company by the relevant foreign registration body; 7. if the company is	of an Australian listed public company; or • licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company.	relevant Australian stock exchange; • a public document issued by the relevant company (for example, annual report); • a search of the relevant ASIC database; or • a search of the license or other records of the relevant Commonwealth, State or Territory regulator.

registered as a private company by the relevant foreign registration body – the name of each Director of the company; and 8. if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.		

(ii) Verification Procedure for all other Australian Companies

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Reliable and Independent Documentation:
1. the full name of the company as registered by the Australian Securities	1. the full name of the company as registered by	A copy of a current: • valid Australian financial services licence issued by ASIC;

and Investments Commission; 2. the full address of the company's registered office; 3. the full address of the company's principal place of business (if any); 4. the ACN issued to the company; 5. whether the company is registered by ASIC as a proprietary or public company; and 6. if the company is registered as a proprietary company, the name of each Director of the company.	the Australian Securities and Investments Commission 2. the ACN issued to the company; and 3. whether the company is registered by ASIC as a proprietary or public company.	• valid company registration certificate issued by ASIC; • in relation to the beneficial ownership of a company, a disclosure certificate that verifies information about the beneficial ownership of a company; or • a disclosure certificate (see Section 47). 2. Reliable and Independent Electronic Data: • ASIC (www.asic.gov.au); • ASX (www.asx.com.au); and • APRA (www.apra.gov.au).
Additional	Additional	
1. all business names used by the company; 2. if the company is a public company, the name	Any other additional information collected.	

of each director of the company; 3. the nature of the business activities conducted by the company; 4. the source of the customer's funds including the origin of funds; 5. the nature and level of the customer's intended transaction behaviour; 6. the name of the company secretary; 7. the name of the Director (if the company is registered as a proprietary company, the name of each director of the company; 8. for an unlisted public company other than an Australian regulated company, the full		

name and address of each Beneficial Owner; 9. in the case of listed companies other than domestic listed companies and companies listed on a recognised foreign stock exchange and their majority owned subsidiaries (approved listed companies) and Australian regulated companies, the full name and address of the Beneficial Owners of the top twenty (20) shareholdings; or 10. details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the company.		

(iii) Verification Procedure for all other ASIC Registered Foreign Companies

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Reliable and Independent Documentation:
1. the full name of the company as registered by ASIC; 2. the full address of the company's registered office in Australia; 3. the full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia (if any); 4. the ARBN issued to the company; 5. the country in which the	1. the full name of the company as registered by ASIC; 2. whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; 3. the ARBN issued to the company.	A copy of a current: • valid Australian financial services licence issued by ASIC; • valid company registration certificate issued by ASIC; • in relation to the beneficial ownership of a company, a disclosure certificate that verifies information about the beneficial ownership of a company; or • a disclosure certificate (only use this if other reliable verification additional information is not reasonably available) – the usage

company was formed, incorporated or registered; 6. whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and 7. if the company is registered as a private company by the relevant foreign registration body - the name of each Director of the company.		of this document requires the AML/CTF CO's approval and the AML/CTF CO will consider the following factors: • ML/TF risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the company; • the jurisdiction of the primary operations of the company and the location of the foreign stock or equivalent exchange (if any); or • the activities undertaken by the company and the availability of evidence about the activities and existence of the company. 2. Reliable and Independent Electronic Data: • a search of the relevant foreign stock or

		equivalent exchange (if any); • a search of the records of the relevant regulator; • ASIC (www.asic.gov.au); • ASX (www.asx.com.au); and • APRA (www.apra.gov.au).
Additional	Additional	
1. all business names used by the company; 2. if the company is a public company, the name of each director of the company; 3. the nature of the business activities conducted by the company; 4. the source of the customer's funds including the origin of funds;	Any other additional information collected.	

5. the nature and level of the customer's intended transaction behaviour; 6. the name of the company secretary; 7. the name of the Director (if the company is registered as a proprietary company, the name of each director of the company; 8. for an unlisted public company other than an Australian regulated company, the full name and address of each Beneficial Owner; 9. in the case of listed companies other than		

domestic listed companies and companies listed on a recognised foreign stock exchange and their majority owned subsidiaries (approved listed companies) and Australian regulated companies, the full name and address of the Beneficial Owners of the top twenty (20) shareholdings; or 10. details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the company.		

(iv) Verification procedure for all other ASIC Unregistered Foreign Companies

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Reliable and Independent Documentation:
1. the full name of the company; 2. the country in which the company was formed, incorporated or registered; 3. whether the company is registered by the relevant foreign registration body and if so: • any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;	1. the full name of the company; 2. whether the company is registered by the relevant foreign registration body and if so: • any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration; • whether it is registered as a	A copy of a current: • valid company registration certificate issued by the relevant foreign registration body; • in relation to the beneficial ownership of a company, a disclosure certificate that verifies information about the beneficial ownership of a company; or • a disclosure certificate (only use this if other reliable verification additional information is not reasonably available) – the usage of this document requires

• the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and • whether it is registered as a private or public company or some other type of company by the relevant foreign registration body; 4. if the company is registered as a private company by the relevant foreign registration body – the name of each Director of the company; and 5. if the company is not registered by the relevant foreign registration body,	private or public company or some other type of company by the relevant foreign registration body.	the AML/CTF CO's approval and the AML/CTF CO will consider the following factors: • ML/TF risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the company; • the jurisdiction of the primary operations of the company and the location of the foreign stock or equivalent exchange (if any); and • the activities undertaken by the company and the availability of evidence about the activities and existence of the company. 2. Reliable and Independent Electronic Data:

the full address of the principal place of business of the company in its country of formation or incorporation.		• a search of the relevant foreign stock or equivalent exchange (if any); and • a search of the records of the relevant regulator.
Additional	Additional	
1. all business names used by the company; 2. if the company is a public company, the name of each director of the company; 3. the nature of the business activities conducted by the company; 4. the source of the customer's funds including the origin of funds; 5. the nature and level of the customer's intended transaction behaviour; 6. the name of the	Any other additional information collected.	

company secretary; 7. the name of the Director (if the company is registered as a proprietary company, the name of each director of the company; 8. for an unlisted public company other than an Australian regulated company, the full name and address of each Beneficial Owner; 9. in the case of listed companies other than domestic listed companies and companies listed on a recognised foreign stock exchange and their majority owned subsidiaries (approved listed companies) and Australian regulated		

companies, the full name and address of the Beneficial Owners of the top twenty (20) shareholdings; 10. details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the company.		

36. TRUSTS: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – CATEGORISATION OF CUSTOMERS

Where a new customer acts in the capacity of a trustee of a trust, it is necessary for CoinPort to be reasonably satisfied that:

(a) the trust exists (refer to Step 2 below); and

(b) the name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided.

Such type of customers can be categorised as one of the following:

(c) regulated trusts; or

(d) other trusts.

STEP 2 – IDENTIFICATION OF THE TYPES OF TRUSTS

Trust Types:

Regulated Trusts	Procedure
(a) a managed investment scheme registered by ASIC	Apply Step 3(i) Simplified verification procedure
(b) a managed investment scheme that is not registered by ASIC, only has wholesale customers and does not make small scale offerings to which section 1012E of the Corporations Act 2001 (Cth) applies	Apply Step 3(i) Simplified verification procedure
(c) registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust	Apply Step 3(i) Simplified verification procedure
(d) a government superannuation fund established by legislation	Apply Step 3(i) Simplified verification procedure

Other Trusts	Procedure
All other trusts that do not fall within the Regulated Trusts category above	Apply Step 3(ii) Verification procedure for all other trusts

Trusts who are Custodians:

An entity:

- acting in the capacity of a trustee;

- providing custodial or depository services as defined by item 46 of table 1 in ss 6(2) of the AML/CTF Act;
- holds an Australian Financial Services Licence authorising it to provide custodial and depository services or is exempt from the requirement to hold such a licence;
- either satisfies one of the geographical link tests in ss 6(6) of the AML/CTF Act or has certified in writing to CoinPort that its name and enrolment details are entered on the Reporting Entities Roll; or
- has certified in writing to CoinPort that it has carried out all applicable KYC and ongoing customer due diligence requirements in accordance with Chapter 15 of the AML/CTF Rules in relation to its underlying customers, prior to, or at the time of becoming a customer of CoinPort.

Procedure: Apply Step 3(iii) Verification procedure for Custodian Trusts.

STEP 3 – IDENTIFICATION AND VERIFICATION PROCEDURES

(i) Simplified verification procedure for Regulated Trusts

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum		
1. the full name (if any) of the trust; 2. the full business name (if any) of the trustee in respect of the trust; 3.	Verify that the trust is one of the following: • a managed investment scheme registered by ASIC; • a managed	1. Verify the information collected by obtaining one or a combination of the

the type of the trust; 4. the country in which the trust was established; 5. the full name of the settlor of the trust, unless: • the material asset contribution to the trust by the settlor at the time the trust is established is less than AUD $10,000.00; or • the settlor is deceased; • the trust is verified using the simplified trustee verification procedure under this Program. 6. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under this Program; 7. if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under this Program; 8. if the trustees comprise of	investment scheme that is not registered by ASIC and that only has wholesale clients and does not make small scale offerings to which section 1012E of the Corporations Act 2001 (Cth) applies; • registered and subject to the regulatory oversight of a commonwealth statutory regulator in relation to its activities as a trust; or • a government superannuation fund established by legislation.	following documents: • a trust deed or extract of the trust deed; • a search of the relevant ASIC, APRA or other regulator database.

individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) is under the applicable customer identification procedures in this Program.		

(ii) Verification Procedure for other Trusts who are not Custodians

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. the full name (if any) of the trust; 2. the full business name (if any) of the trustee in respect of the trust; 3. the type of the trust; 4. the country in which the trust was established; 5. the full name of the settlor of	1. the full name of the trust; 2. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under this Program; 3. if any	• a trust deed, certified copy or certified extract of a trust deed; • reliable and independent documentation relating to the trust; and/or • reliable and independent electronic data. • For trustees (individuals or

the trust, unless: • the material asset contribution to the trust by the settlor at the time the trust is established is less than AUD $10,000.00; or • the settlor is deceased; or • the trust is verified using the simplified trustee verification procedure under this Program. 6. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under this Program; 7. if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under this Program; 8. if the trustees comprise of individuals and companies then in respect of either an individual or a company – the	of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under this Program; 4. if the trustees comprise of individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) is under the applicable customer identification procedures in this Program. 5. the full name of the settlor of the trust, unless: • the material asset contribution to the trust by the settlor at the time the trust is established is less than AUD $10,000.00; or • the settlor is deceased; or • the trust is verified using the simplified trustee	companies) please refer to Section 37 below.

information required to be collected from the individual or company (as the case may be) is under the applicable customer identification procedures in this Program.	verification procedure under this Program.	
Additional	Additional	
1. all business names used by the trusts and any other name under which the trust operates; 2. the nature of the business activities conducted by the trust; 3. the source of the customer's funds including the origin of funds; 4. the jurisdiction in which the trust was established; 5. details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the trust; 6. the nature and level of the customer's intended	Any other additional information collected.	

transaction behaviour; 7. the income and assets (including location) of the trust; and 8. details of any parties with which the trust owns property, is in partnership or undertakes a joint venture.		

(iii) Verification Procedure for Trusts who are Custodians

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. the full name (if any) of the trust; 2. the full business name (if any) of the trustee in respect of the trust; 3. the type of the trust; 4. the country in which the trust was established; 5. the full name of the settlor of the trust, unless: • the material asset contribution to the trust by the settlor at	1. the full name of the trust; 2. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under this Program; 3. if any of the trustees is a company, then in respect of one of those companies – the	• a trust deed, certified copy or certified extract of a trust deed; • obtain confirmation in writing that its name and enrolment details are entered on the Reporting Entities Roll; • obtain confirmation in writing that it has carried out all applicable KYC and ongoing customer due diligence requirements

the time the trust is established is less than AUD $10,000.00; or • the settlor is deceased; or • the trust is verified using the simplified trustee verification procedure under this Program; and 6. The Australian Financial Services Licence number of the trust.	information required to be collected from a company under this Program; 4. if the trustees comprise of individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) is under the applicable customer identification procedures in this Program. 5. the full name of the settlor of the trust, unless: • the material asset contribution to the trust by the settlor at the time the trust is established is less than AUD $10,000.00; or • the settlor is deceased; or • the trust is verified using the simplified trustee verification procedure under this Program; 6. The Australian Financial Services	in accordance with Chapter 15 of the AML/CTF Rules in relation to its underlying customers, prior to, or at the time of becoming a customer of CoinPort; • reliable and independent documentation relating to the trust; and/or • reliable and independent electronic data.

	Licence number and authorisation of the trust; 7. either satisfies one of the geographical link tests in ss 6(6) of the AML/CTF Act or that its name and enrolment details are entered on the Reporting Entities Roll; and 8. that it has carried out all applicable KYC and ongoing customer due diligence requirements in accordance with Chapter 15 of the AML/CTF Rules in relation to its underlying customers, prior to, or at the time of becoming a customer of CoinPort.	
Additional	Additional	
1. all business names used by the trusts and any other name under which the trust operates; 2. the nature of the business activities conducted by the trust; 3. the source of the customer's funds	Any other additional information collected.	

including the origin of funds; 4. the jurisdiction in which the trust was established; 5. details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the trust; 6. the nature and level of the customer's intended transaction behaviour; 7. the income and assets (including location) of the trust; and 8. details of any parties with which the trust owns property, is in partnership or undertakes a joint venture.		

37. TRUSTEES AND BENEFICIARIES: CUSTOMER IDENTIFICATION AND VERIFICATION

IDENTIFICATION AND VERIFICATION PROCEDURES

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Verify	
1. the full name and address of each trustee in respect of the trust; and 2. either the: • full name of each beneficiary of the trust; or • if the terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.	1. if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under this Program; 2. if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under this Program; 3. if the trustees comprise of individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) is under the applicable customer	1. Individuals – refer to the verification procedures at Section 34. 2. Companies – refer to the verification procedures at Section 35.

	identification procedures in this Program.	

38. PARTNERSHIPS: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – EXISTENCE OF A PARTNERSHIP

Where a new customer is a partnership, it is necessary for CoinPort to be reasonably satisfied that:

1. the partnership exists; and
2. the name for each of the partners in the partnership has been provided in accordance with point 4 under "KYC information to be collected" in step 2 below.

STEP 2 – IDENTIFICATION AND VERIFICATION PROCEDURES

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. full name of the partnership; 2. the full business name (if any) of the partnership as registered under any State or Territory business names legislation 3. the country in which the	1. full name of the partnership; 2. in respect of one of the partners – the information required to be collected under Section 34.	• a partnership agreement, certified copy or certified extract of a partnership agreement; • a certified copy or certified extract of minutes of a partnership meeting; • reliable and

partnership was established; 4. in respect of one of the partners – the information required to be collected under Section 34 of this Program; and 5. the full name and residential address of each partner in the partnership except where the regulated status of the partnership is confirmed through reference to the current membership directory of the relevant professional association.		independent documentation relating to the partnership; and/or • reliable and independent electronic data.
Additional	Additional	
1. any alias names used by the partner; 2. the partnership's business activities; 3. the source of the partnership's funds including the origin of funds; 4. income and assets of the partnership; 5. the nature and level of the partnership's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the partnership/the partnership's account with CoinPort. *Note: The	Any other additional information collected.	

information collection requirements are not intended to conflict with any other obligation CoinPort has under other legislation including the Privacy Act 1988. Any conflicts, which arise, should be immediately notified to the AML/CTF CO.		

39. ASSOCIATIONS: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – EXISTENCE OF AN ASSOCIATION

Where a new customer is an association, it is necessary for CoinPort to be reasonably satisfied that:

1. the association exists; and
2. the name for any members of the governing committee (howsoever described) of the association have been provided.

STEP 2 – CATEGORISATION OF ASSOCIATIONS

Types of Associations:

| Incorporated Associations | Apply Step 3(i) Verification procedure for incorporated associations |
| Unincorporated Associations | Apply Step 3(ii) Verification procedure for unincorporated associations |

STEP 3 – IDENTIFICATION AND VERIFICATION PROCEDURES

(i) Verification procedure for Incorporated Associations

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. the full name of the association; 2. the full address of the association's principal place of administration or registered office (if any) or the residential address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer; 3. any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association; and 4. the full name of the chairman, secretary and	1. the full name of the association; and 2. any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association.	• the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association; • the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association; • in the case of an incorporated association, information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association; • reliable and

treasurer or equivalent officer in each case of the association.		independent documentation relating to the association; and/or • reliable and independent electronic data.
Additional	Additional	
1. any alias names used by the member of the association; 2. the association's business activities; 3. the source of the association's funds including the origin of funds; 4. income and assets of the association; 5. the nature and level of the association's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the member/the association's account with CoinPort. *Note: The information collection requirements are not intended to conflict with any other obligation CoinPort has under other legislation including the Privacy Act	Any other additional information collected.	

1988. Any conflicts, which arise, should be immediately notified to the AML/CTF CO.		

(ii) Verification Procedure for Unincorporated Association

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the full name of the association with one of the following documents:
1. the full name of the association; 2. the full address of the association's principal place of administration (if any); 3. the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and 4. in respect of the member – the information required to be collected from an individual under the applicable customer identification procedure in accordance with Section 34 of this Program.	1. the full name of the association; 2. in respect of the member – the information required to be collected from an individual under the applicable customer identification procedure in accordance with Section 34 of this Program.	• the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association; or • the minutes of meeting of the association or a certified copy or certified extract of any minutes of meeting of the association. • For beneficial owners and signatories – verify beneficial owners and signatories in accordance with the

		KYC procedure for individuals as per Section 34.
Additional	Additional	
1. any alias names used by the member of the association; 2. the association's business activities; 3. the source of the association's funds including the origin of funds; 4. income and assets of the association; 5. the nature and level of the association's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the member/the association's account with CoinPort.	Any other additional information collected.	

40. REGISTERED CO-OPERATIVES: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – EXISTENCE OF A REGISTERED CO-OPERATIVE

Where a new customer is a registered co-operative, it is necessary for CoinPort to be reasonably satisfied that:

1. the co-operative exists; and
2. the name for the chairman, secretary or equivalent in each case of the co-operative have been provided.

STEP 2 – IDENTIFICATION AND VERIFICATION PROCEDURES

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. the full name of the co-operative; 2. the full address of the co-operative's registered office or principal place of operations (if any) or the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer; 3. any unique identifying number issued to the co-operative upon its registration by the State, Territory or overseas body responsible for the registration of the co-operative; and 4. the full name of the	1. the full name of the co-operative; and 2. any unique identifying number issued to the co-operative upon its registration by the state, territory or overseas body responsible for the registration of the co-operative.	• any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative; • the minutes of meeting of the co-operative or a certified copy or certified extract of minutes of meeting of the co-operative; • information provided by the State, Territory or overseas body responsible for the registration of the co-operative;

chairman, secretary and treasurer or equivalent officer in each case of the co-operative.		• reliable and independent documentation relating to the co-operative; or • reliable and independent electronic data.
Additional	Additional	
1. any alias names used by the member of the co-operative; 2. the co-operative's business activities; 3. the source of the co-operative's funds including the origin of funds; 4. income and assets of the co-operative; 5. the nature and level of the co-operative's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the member/the co-operative's account with CoinPort. *Note: The information collection requirements are not intended to conflict with any other obligation CoinPort has under other legislation	Any other additional information collected.	

including the Privacy Act 1988. Any conflicts, which arise, should be immediately notified to the AML/CTF CO.		

41. GOVERNMENT BODIES: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – EXISTENCE OF A GOVERNMENT BODY

Where a new customer is a government body, it is necessary for CoinPort to be reasonably satisfied that:

1. the government body exists; and
2. in the case of certain kinds of government bodies – information about the beneficial owners of the government body.

STEP 2 – CATEGORISATION OF GOVERNMENT BODIES

Types of Government Bodies:

| Australian Government Body | Apply Step 3(i) Verification procedure for Australian Government Body |
| Foreign Government Body | Apply Step 3(ii) Verification procedure for Foreign Government Body |

STEP 3 – IDENTIFICATION AND VERIFICATION PROCEDURES

(i) Verification Procedure for Australian Government Body

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:

1. Full name of the government body; 2. Full address of the government body's principal place of operations; 3. Whether the government body is an entity or emanation, or is established under legislation of the Commonwealth; and 4. Whether the government body is an entity or emanation or is established under legislation of a state or territory; and if so the name of the state or territory.	1. Full name of the government body 2. Full address of the government body's principal place of operations 3. Whether the government body is an entity or emanation, or is established under legislation of the Commonwealth; and 4. Whether the government body is an entity or emanation, or is established under legislation of a state or territory; and if so the name of the state or territory	• government directories search; • government/regulatory authorities search summary; • register of government bodies extract; and/or • a legislative extract establishing the body.
Additional	Additional	
1. any alias names used by the member of the government body; 2. the government body's business activities; 3. the source of the government body's funds including the origin of funds; 4. income and assets of	Any other additional information collected	

the government body; 5. the nature and level of the government body's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the member/the government body's account with CoinPort.		

(ii) Verification Procedure for Foreign Government Body

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
Minimum	Minimum	1. Verify the information collected with one or a combination of the following documents:
1. Full name of the government body; 2. Full address of the government body's principal place of operations; 3. Whether the government body is an entity or emanation, or is	1. Full name of the government body; 2. Full address of the government body's principal place of operations; 3. Whether the government body is an entity or emanation, or is	• government directories search; • government / regulatory authorities search summary; • register of

established under legislation of the foreign country; and if so the name of the foreign country; and 4. Beneficial Owners: should be identified and verified in accordance with the KYC procedure for individuals (with the exception of occupation/industry information).	established under legislation of the foreign country; and if so the name of the foreign country; and 4. Beneficial Owners: should be identified and verified in accordance with the KYC procedure for individuals (with the exception of occupation/industry information).	government bodies extract; or • a legislative extract establishing the body. • Verify Beneficial Owners in accordance with Section 34.
Additional	Additional	
1. any alias names used by the member of the government body; 2. the government body's business activities; 3. the source of the government body's funds including the origin of funds; 4. income and assets of the government body; 5. the nature and level of the government body's intended transaction behaviour; and 6. the beneficial ownership of the funds used by the	Any other additional information collected.	

member/the government body's account with CoinPort.		

42. AGENTS: CUSTOMER IDENTIFICATION AND VERIFICATION

STEP 1 – EXISTENCE OF AN AGENT

Where a customer authorises an agent to act for or on behalf of them in relation to a designated service, it is necessary for CoinPort to be reasonably satisfied that:

1. the agent exists; and
2. the authorisation is able to be evidenced.

STEP 2 – IDENTIFICATION AND VERIFICATION PROCEDURES

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect to Verify KYC Information
1. Full name of each agent acting on the customer's behalf; and 2. Evidence of the authorisation of the agent to act on behalf of the customer.	Only verify the agent if there are doubts as to the veracity of the information supplied by the customer, in accordance with the KYC procedures for individuals	Verify in accordance with the KYC procedure for individuals (refer to Section 34).

43. BENEFICIAL OWNERS

STEP 1 – DETERMINING THE BENEFICIAL OWNER OF EACH CUSTOMER

43.1 In identifying Beneficial Owners of a customer, CoinPort may:

- (a) collect from the customer information relating to the ownership structure of the customer including but not limited to:
    - information relating to shareholders of the company;
    - information relating to people exercising responsibility for senior management decisions;
    - information relating to people with the ability to control the customer and/or dismiss or appoint those in senior management positions;
    - information relating to those people holding more than 25% of the customer's rights;
    - information relating to those individuals who hold senior management positions;
    - trustees (where applicable);
- (b) if the customer is controlled by other entities (and/or those entities are in turn controlled by further entities) the ownership structure of each entity must also be clarified until CoinPort has a clear understanding of who the ultimate Beneficial Owners are.

43.2 CoinPort's employees are required to identify and verify each customer's beneficial owners subject to the exceptions below.

43.3 If CoinPort is unable to ascertain a Beneficial Owner, the reporting entity must identify and take reasonable measures to verify:

- (a) for a company (other than a company verified under simplified company verification procedure or a partnership), any individual who:
    - is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including power to veto, or
    - holds the position of senior managing official (or equivalent);
- (b) for a trust (other than a trust verified under simplified verification procedure), any individual who holds the power to appoint or remove the trustees of the trust;
- (c) for an association or a registered co-operative, any individual who:
    - is entitled (either directly or indirectly) to exercise 25% or more of the voting rights including a power of veto, or
    - would be entitled on dissolution to 25% or more of the property, or
    - holds the position of senior managing official (or equivalent).

EXCEPTIONS

43.4 CoinPort does not need to identify and verify its customer's beneficial owners if the customer is:

- an individual - CoinPort may assume that the customer and the Beneficial Owner are one and the same, unless CoinPort has reasonable grounds to consider otherwise;
- a company verified under 'Simplified Verification Procedures';
- a trust verified under 'Simplified Verification Procedures'; or
- a foreign listed public company subject to disclosure requirements to ensure transparency of beneficial ownership which are, or are comparable to, the requirements in Australia.

STEP 2 – IDENTIFICATION AND VERIFICATION PROCEDURES

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect
Minimum	Minimum	Verify in accordance with KYC procedure for individuals (refer to Section 34)
1. each Beneficial Owner's full name, and	1. each Beneficial Owner's full name, and	
2. Beneficial Owner's date of birth; or	2. Beneficial Owner's date of birth; or	
3. Beneficial Owner's full residential address	3. Beneficial Owner's full	

	residential address	
Additional	Additional	
1. Beneficial Owner's former name(s)	Any other additional information collected	
2. Beneficial Owner's occupation or business activities		
3. source of Beneficial Owner's funds including origin of funds		
4. income and assets of Beneficial Owner		
5. nature and level of Beneficial Owner's intended transaction behaviour		
6. beneficial ownership of funds used by Beneficial Owner		
7. details of Beneficial Owner's employment		

44. POLITICALLY EXPOSED PERSONS

STEP 1 – EXISTENCE OF A POLITICALLY EXPOSED PERSON

If when conducting the risk analysis of a customer, CoinPort has a reasonable suspicion that a customer is a Politically Exposed Person ("PEP"), the AML/CTF CO must conduct in relation to that customer additional checks to determine whether the

customer is a PEP. These checks might include but are not limited to:

1. a customer self-declaration regarding their PEP status;
2. an internet and media search;
3. a search of relevant commercial databases (if available to CoinPort);
4. Government issued PEP lists relevant to the jurisdiction/s of the customer;
5. Information sharing databases relating to PEP within the Australian financial system; and
6. asset disclosure systems.

STEP 2 – CATEGORISATION OF PEPS

Types of PEPs	
Australian PEP	Apply Step 3(i) Verification Procedure for Australian/International Organisation PEPs
International Organisation PEP	
Foreign PEP	Apply Step 3(ii) Verification Procedure for Foreign PEPs

STEP 3 – IDENTIFICATION AND VERIFICATION PROCEDURES

(i) Verification Procedure for Australian/International Organisation PEPs

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect
Minimum	Minimum	Verify in accordance with KYC procedure for

		individuals (refer to Section 34)
1. Full name	1. Name; and	
2. Residential address; and	2. Residential address or date of birth	
3. Date of Birth		
Additional	Additional	
1. PEP's former name(s)	Any other additional information collected	
2. PEP's occupation or business activities		
3. source of PEP's funds including origin of funds		
4. income and assets of PEP		
5. details of PEP's employment		

STEP 4 – RISK ASSESSMENT OF THE PEP

Determine whether the PEP is of high money laundering or terrorism financing risk.

If the customer is determined to be of high money laundering or terrorism financing risk, then, in addition to Step 3 above:

1. obtain the Board's approval before establishing or continuing a business relationship with the individual and before the provision, or continued provision, of a designated service to the customer; and

2. take reasonable measures to establish the PEP's source of wealth and source of funds; and
3. comply with the ongoing due diligence obligations.

(ii) Verification Procedure for Foreign PEPs

KYC Information to be Collected	KYC Information to be Verified	Documents to Collect
Minimum	Minimum	Verify in accordance with KYC procedure for individuals (refer to Section 34)
1. Full name	1. Name; and	
2. Residential address; and	2. Residential address or date of birth	
3. Date of Birth		
Additional	Additional	
1. PEP's former name(s)	Any other additional information collected	
2. PEP's occupation or business activities		
3. source of PEP's funds including origin of funds		
4. income and assets of PEP		
5. details of PEP's employment		

STEP 4 – FURTHER ACTION

1. obtain the Board's approval before establishing or continuing a business relationship with the individual and before the provision, or continued provision, of a designated service to the customer;
2. take reasonable measures to establish the PEP's source of wealth and source of funds; and
3. comply with the ongoing due diligence obligations.

45. NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF CO

45.1 The AML/CTF CO must be notified of all new customers prior to the provision of any services.

45.2 Sign-off for each new customer should be obtained from the AML/CTF CO certifying that no additional KYC Information relating to the customer's existence needs to be verified.

46. TOLERANCE OF DISCREPANCIES AND ERRORS

46.1 Tolerance of discrepancies: Where, during the KYC Information collection and verification process, a director, officer or employee of CoinPort discovers any discrepancies in the KYC Information provided by the new customer, the matter should be immediately notified to the AML/CTF CO. The discrepancy must not be raised with the new customer without first consulting the AML/CTF CO.

46.2 The AML/CTF CO must then collect from the customer whatever additional information they consider necessary to verify that the customer is the person that they claim they are.

46.3 Pre-defined tolerance levels for matches and errors: CoinPort will allow for obvious typographical errors in customer information other than name, company registration or identification number, or date of birth. Where the error relates to name, company registration or identification number, or date of birth, the AML/CTF CO should be notified and independent contact should be initiated with the customer to clarify the information.

47. DISCLOSURE CERTIFICATES

47.1 Disclosure certificates may only be requested from customers in the following circumstances:

(a) CoinPort has determined that the information cannot otherwise be reasonably obtained or verified;

(b) the information to be provided or verified is reasonably required under this Program;

(c) CoinPort has applied the relevant procedures and requirements of this Program, but has been unable to obtain or verify the information; and

(d) the information is one or more of the items specified below.

Note: Disclosure certificates are typically used for complex corporate structures, foreign entities, or trusts where standard verification methods are insufficient. The AML/CTF CO must approve all requests for disclosure certificates.

APPENDICES

APPENDIX 1 – LIST OF CERTIFIERS

A certified copy means a document that has been certified as a true copy of an original document by one of the following persons:

(a) a person who, under a law in force in a State or Territory, is currently licensed or registered to practise in an occupation listed in Part 1 of Schedule 2 of the Statutory Declarations Regulations 2018;

(b) a person who is enrolled on the roll of the Supreme Court of a State or Territory, or the High Court of Australia, as a legal practitioner (however described);

(c) a person listed in Part 2 of Schedule 2 of the Statutory Declarations Regulations 2018. For the purposes of these Rules, where Part 2 uses the term '5 or more years of continuous service', this should be read as '2 or more years of continuous service';

(d) an officer with, or authorised representative of, a holder of an Australian financial services licence, having 2 or more years of continuous service with one or more licensees;

(e) an officer with, or a credit representative of, a holder of an Australian credit licence, having 2 or more years of continuous service with one or more licensees;

(f) a person in a foreign country who is authorised by law in that jurisdiction to administer oaths or affirmations or to authenticate documents.

APPENDIX 2 – RED FLAG INDICATORS SHEET

Purpose: This sheet must be completed for each new customer during onboarding and reviewed semi-annually for existing customers, or whenever the AML/CTF Compliance Officer deems necessary.

Instructions: Check any boxes that apply. One or more red flags triggers enhanced due diligence procedures (Section 22).

CUSTOMER BEHAVIOR RED FLAGS

□ Reluctant to provide identification - Customer hesitant, evasive, or refuses to provide required KYC documents

□ Suspicious identification documents - Documents appear altered, fake, or inconsistent with other information provided

□ Nervous or evasive behavior - Customer exhibits unusual anxiety when asked routine questions

□ 55+ age with limited crypto knowledge (Fraud Prevention - Section 32.9) - Older customer with little understanding of cryptocurrency, potential fraud victim

□ Multiple accounts or wallets - Customer attempts to open multiple accounts or uses multiple wallets for no clear reason

□ Requests services below reporting thresholds - Consistently structures transactions just under $10,000 AUD

□ Occupation inconsistent with transaction patterns - Customer's stated employment doesn't match transaction volumes or frequency

□ Requests unusual secrecy - Customer asks for confidentiality beyond normal privacy expectations

□ Coached responses - Customer appears to be reading from a script or receiving instructions from another person

□ Uses VPN to obscure location - Systematic use of VPN or anonymization services during platform access

□ Multiple failed KYC attempts - Repeated KYC submission failures with different details

---

TRANSACTION PATTERN RED FLAGS

□ Rapid fund movement - Immediate deposit followed by quick withdrawal to different wallet

□ Round number transactions - Transactions in exact amounts ($5,000, $10,000, $50,000)

□ Threshold avoidance - Pattern of transactions consistently just below $10,000 TTR threshold

□ Sudden 100%+ volume increase - Transaction volume doubles within 5 calendar days (Section 30.6(b)(v))

□ High-frequency inconsistent with profile - Trading frequency doesn't match stated occupation, income, or experience level

□ Complex transaction chains - Unnecessarily complicated series of transactions with no clear economic rationale

□ Transactions with high-risk jurisdictions - Regular transfers to/from countries on FATF high-risk list or sanctioned jurisdictions

□ Unusual cross-border patterns - Geographic transaction patterns inconsistent with customer profile

□ Transactions involving PEPs - Customer transacting with known Politically Exposed Persons

□ Large cash deposits - Customer prefers large cash-to-crypto conversions over traceable bank transfers

□ No clear commercial purpose - Transactions have no logical business or personal rationale

□ Inconsistent transaction behavior change - Significant, unexplained change in normal transaction patterns

---

BLOCKCHAIN ANALYTICS RED FLAGS

□ Deposits from mixers/tumblers - Funds received from Tornado Cash, Wasabi Wallet, CoinJoin, or similar mixing services flagged by AMLBot

□ High-risk wallet tagging - Wallet flagged by AMLBot as high-risk or associated with illicit activity

□ Darknet market links - Direct or indirect connection to darknet marketplace addresses detected by AMLBot

□ Sanctioned address interaction - Wallet has transacted with OFAC SDN, DFAT Consolidated List, or UN sanctions addresses (AMLBot alert)

□ Blacklisted exchange interaction - Deposits from or withdrawals to exchanges flagged by AMLBot as non-compliant or high-risk

□ Exchange hop patterns - Funds rapidly moved through multiple exchanges in short timeframe

□ P2P exchange suspicious activity - Wallet associated with suspicious P2P exchange patterns

□ Ransomware connections - Wallet linked to known ransomware payment addresses (AMLBot flagged)

□ Theft/hack associations - Funds traceable to known exchange hacks or theft incidents (AMLBot flagged)

□ Recent mixing service use - Interaction with mixing services in past 7 days detected by AMLBot

□ High-risk jurisdiction wallets - AMLBot identifies wallet addresses associated with sanctioned jurisdictions (North Korea, Iran, etc.)

□ Privacy coin conversions - Regular conversion to/from privacy coins (Monero, Zcash)

TRAVEL RULE RED FLAGS (Effective 31 March 2026)

□ Incomplete originator information - VASP-to-VASP transfer missing required originator details (ANY amount)

□ Non-responsive counterparty VASP - Beneficiary VASP fails to respond to Travel Rule messages after 3 attempts/24 hours

□ Geographic inconsistencies - Australian customer sending to VASP in high-risk or sanctioned jurisdiction

□ Counterparty VASP not on approved list - Receiving VASP not verified through AUSTRAC, Notabene, or TRISA directories

□ Customer unable to provide beneficiary VASP info - Customer cannot identify which VASP they're sending to

□ Inconsistent Travel Rule data - Originator/beneficiary information conflicts with known customer data

□ Frequent high-value self-hosted transfers - Regular transfers ≥$10,000 AUD to self-hosted (unhosted) wallets

□ VASP counterparty sanctions hit - Beneficiary VASP appears on sanctions lists or has regulatory warnings

□ Travel Rule data quality issues - Systematic formatting errors or incomplete fields in Travel Rule messages

□ Unusual VASP-to-VASP patterns - High frequency of VASP transfers inconsistent with customer profile

CORPORATE/TRUST/ENTITY CUSTOMER RED FLAGS

□ Complex ownership structure - Multiple layers of companies/trusts with no clear commercial rationale

□ Offshore entities - Company or trust incorporated in tax haven or secrecy jurisdiction

□ Beneficial ownership unclear - Cannot identify ultimate individual beneficial owners despite reasonable efforts

□ Nominee directors/shareholders - Use of professional nominees obscuring true ownership

□ Recently incorporated shell company - New company with minimal business activity seeking large transactions

□ Cash-intensive business - Customer operates business involving significant cash transactions

□ No clear business purpose - Company or trust exists with no obvious legitimate business activity

□ Frequent ownership changes - Multiple changes in directors, shareholders, or beneficial owners within short period

□ Inconsistent corporate documents - Trust deeds, company constitutions, or partnership agreements contain inconsistencies

□ Reluctant to provide corporate documents - Customer hesitant to provide trust deed, shareholder register, or company records

□ SMSF red flags - SMSF without proper ATO registration, unusual trustee arrangements, or pension phase irregularities

□ Related party transactions - Unusual transactions between related companies/trusts with no commercial justification

□ Dormant company suddenly active - Long-dormant company suddenly conducting high-value cryptocurrency transactions

□ Business address is virtual office - Company registered at mail forwarding service or virtual office

□ Industry inconsistent with crypto use - Traditional business with no clear reason for cryptocurrency transactions

---

SOURCE OF FUNDS RED FLAGS

□ Cannot verify source of funds - Customer unable or unwilling to document origin of cryptocurrency or fiat funds

□ Inconsistent source of wealth - Declared income/assets don't match transaction volumes

□ Non-employment income - Income from sources that are difficult to verify (gambling, gifts, inheritance with no documentation)

□ Offshore funds access - Customer has unexplained access to offshore accounts or funds

□ Recent large inheritance or windfall - Sudden wealth with minimal documentation

□ Self-employed with complex income - Self-employment income that is difficult to verify or document

---

HIGH-RISK JURISDICTION RED FLAGS

□ Customer based in high-risk jurisdiction - Customer resident in or operating from FATF high-risk or non-cooperative jurisdiction

□ Transactions with high-risk countries - Regular transfers to/from countries with weak AML/CTF frameworks

□ Sanctioned country connections - Any connection to countries under Australian, UN, OFAC, or EU sanctions

□ Proliferation financing risk jurisdictions - Links to countries of WMD proliferation concern (North Korea, Iran)

□ No local operations - Customer claims business in foreign jurisdiction but has no verifiable presence

---

PROLIFERATION FINANCING (PF) RED FLAGS

□ Jurisdictions of PF concern - Customer or transaction involving North Korea, Iran, or other jurisdictions subject to WMD-related sanctions

□ Dual-use goods involvement - Customer's business involves chemicals, metals, technology, or other items with both civilian and military applications

□ Front company indicators - Corporate structure appears designed to obscure true ownership or purpose, particularly with links to high-risk jurisdictions

□ Sanctions evasion patterns - Complex transaction routing or corporate structures that appear designed to evade international sanctions

□ Shell company networks - Multiple related entities with minimal business activity and opaque ownership in different jurisdictions

□ State-owned enterprise connections - Links to state-owned companies in jurisdictions of PF concern

□ Technology/scientific sector - Customer involved in advanced technology, scientific research, or manufacturing with potential WMD applications

□ Unusual shipping/logistics - Business involves complex international shipping arrangements inconsistent with stated business purpose

□ Academic/research institution links - Connections to research institutions in jurisdictions of PF concern, particularly in nuclear, chemical, or biological fields

□ Sanctioned entity associations - Customer has business relationships or transactions with entities on UN, OFAC, or DFAT proliferation-related sanctions lists

---

POLITICALLY EXPOSED PERSON (PEP) RED FLAGS

□ Customer identified as PEP - Customer holds or has held prominent public office (domestic, foreign, or international organization)

□ Family member of PEP - Customer is immediate family member of a PEP

□ Close associate of PEP - Customer has close business or personal relationship with a PEP

□ Adverse media on PEP - Negative media coverage relating to corruption, financial crime, or misconduct

---

FRAUD VICTIM INDICATORS (Section 32.9)

□ Romance scam indicators - Customer mentions online relationship, requests to send crypto to “partner”

□ Investment scam indicators - Customer directed to invest in “guaranteed return” crypto schemes

□ Pressure to send funds urgently - Customer expresses urgency to complete transaction due to external pressure

□ Limited understanding with large transactions - Customer wants to send large amounts but has minimal crypto knowledge

□ Instructions from third party - Customer receiving step-by-step instructions from someone else

□ Isolation from family/friends - Customer mentions keeping crypto activities secret from family

---

SANCTIONS SCREENING RED FLAGS

□ DFAT Consolidated List match - Customer name match on Australian sanctions list
□ UN Security Council sanctions match - Match on UN sanctions list
□ OFAC SDN match - Match on US OFAC Specially Designated Nationals list (where applicable)
□ EU/UK sanctions match - Match on European Union or UK HM Treasury sanctions lists
□ Proliferation financing sanctions - Match on WMD proliferation-related sanctions designations

---

ACTIONS REQUIRED WHEN RED FLAGS IDENTIFIED

1 Red Flag:

- Employee completes enhanced due diligence
- Reports to immediate supervisor
- Supervisor reports to AML/CTF Compliance Officer with findings
- AML/CTF CO assesses whether SMR required

Multiple Red Flags (2+):

- Immediate escalation to AML/CTF Compliance Officer
- Enhanced due diligence mandatory
- Consider suspending transaction pending investigation
- Document all findings comprehensively
- Likely SMR submission required

Critical Red Flags (Sanctions, Darknet, Ransomware):

- Immediate transaction hold
- Escalate to AML/CTF CO within 1 hour
- Senior management notification
- SMR likely required within 24 hours (terrorism financing) or 3 business days (other)
- Consider account suspension

Customer
Name: _____
Account
Number: _____
Date
Completed: _____
Completed By: _____
Red Flags Identified: _____ (number)
Action Taken: _____
AML/CTF CO
Review: _____
SMR Filed: □ Yes □ No Date: _____

APPENDIX 3 – RISK ASSESSMENT AND MANAGEMENT MATRIX

INTRODUCTION

This Risk Assessment Matrix identifies CoinPort's specific ML/TF/PF risks across four key categories and documents the controls in place to mitigate these risks. This matrix is reviewed quarterly by the AML/CTF Compliance Officer and updated following any adverse event or material business change.

Risk Scoring Methodology:

- Likelihood: LOW (1) | MEDIUM (2) | HIGH (3)
- Impact: LOW (1) | MEDIUM (2) | HIGH (3)
- Overall Risk Score: Likelihood × Impact = Score (1-9)
- Risk Rating: LOW (1-3) | MEDIUM (4-6) | HIGH (7-9)

---

1. CUSTOMER TYPE RISK ASSESSMENT

Individual Australian Retail Customer (Standard Profile)

Profile: Australian resident, employment income, standard transaction volumes (<$10,000/month), no PEP status, no high-risk jurisdiction connections

Risk Factor	Assessment
Likelihood	LOW (1) - Know Your Customer, local regulation, verifiable income
Impact	LOW (1) - Limited transaction volumes, retail amounts, full KYC

Overall Risk Score	1 (LOW)

Controls:

- Standard KYC verification via KYC-AID or Sumsub
- Electronic ID verification with liveness detection
- Annual KYC review and refresh
- Automated transaction monitoring
- Sanctions screening at onboarding and daily (customer-level)
- AMLBot blockchain analytics on all deposits/withdrawals (wallet-level screening)
- Real-time screening for sanctioned addresses, blacklisted exchanges, and high-risk counterparties
- 55+ age fraud screening (Section 32.9)

Monitoring Frequency: Annual KYC review, automated transaction monitoring

---

Individual Customer - Medium Risk Profile

Profile: Self-employed, higher transaction volumes ($10,000-$50,000/month), cross-border remittances, income verification more complex

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Income harder to verify, higher volumes, cross-border activity
Impact	MEDIUM (2) - Larger transaction amounts, potential for structured transactions
Overall Risk Score	4 (MEDIUM)

Controls:

- Standard KYC plus additional source of funds documentation
- Occupation/business verification
- Enhanced transaction monitoring (weekly review)
- Semi-annual KYC refresh
- Source of wealth documentation for large deposits
- Additional scrutiny on cross-border transactions
- Blockchain analytics with manual review of flagged transactions

Monitoring Frequency: Semi-annual KYC review, weekly transaction monitoring

---

Individual Customer - High Risk Profile (PEP)

Profile: Politically Exposed Person (domestic, foreign, or international organization), potential for corruption, higher reputational risk

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Enhanced scrutiny target, higher regulatory attention
Impact	HIGH (3) - Severe reputational damage if ML/TF occurs, regulatory sanctions
Overall Risk Score	6 (MEDIUM-HIGH)

Controls:

- Enhanced CDD mandatory (Section 44)
- Senior management approval before account opening
- Source of wealth and source of funds verification required
- Semi-annual KYC review with AML/CTF CO sign-off
- Enhanced transaction monitoring (weekly review by AML/CTF CO)
- Real-time sanctions screening
- Board notification of PEP customer relationships
- Adverse media screening quarterly

Monitoring Frequency: Semi-annual KYC review, weekly enhanced transaction monitoring

---

Individual Customer - Prohibited/Very High Risk

Profile: Customer in sanctioned jurisdiction, known criminal associations, unable to verify identity, privacy coin enthusiast

Risk Factor	Assessment
Likelihood	HIGH (3)
Impact	HIGH (3)
Overall Risk Score	9 (HIGH) - PROHIBITED

Controls:

- ACCOUNT OPENING REFUSED
- Existing accounts immediately suspended upon identification
- Immediate SMR filing
- Funds frozen pending regulatory guidance
- Board and AUSTRAC notification

Corporate/Trust/Partnership Customers

Profile: Companies, trusts, partnerships, SMSFs, institutional clients requiring beneficial ownership verification

Risk Factor	Assessment
Likelihood	MEDIUM (2) - More complex structures, beneficial ownership verification required
Impact	MEDIUM (2) - Larger transaction volumes, potential for shell companies
Overall Risk Score	4 (MEDIUM)

Controls:

- Enhanced KYC procedures per Sections 35-42
- Beneficial ownership verification to ultimate individual level (25% threshold)
- Corporate structure analysis
- Enhanced sanctions screening (entity + beneficial owners)
- Source of funds verification
- Annual KYC review minimum
- Enhanced transaction monitoring
- Red flag screening for shell company indicators
- PF-specific screening for dual-use goods and sanctions evasion

Monitoring Frequency: Annual KYC review minimum (more frequent for higher-risk entities), enhanced transaction monitoring

Corporate/Trust Customers - Prohibited/Very High Risk

Profile: Shell companies with no genuine business, offshore trusts in secrecy jurisdictions, entities refusing beneficial ownership disclosure, sanctioned entities

Risk Factor	Assessment
Likelihood	HIGH (3)
Impact	HIGH (3)
Overall Risk Score	9 (HIGH) - PROHIBITED

Controls:

- ACCOUNT OPENING REFUSED
- Existing accounts immediately suspended upon identification
- Immediate SMR filing
- Beneficial ownership disclosure mandatory - refusal = account rejection
- Enhanced screening for shell company indicators
- Sanctions screening of all corporate entities and beneficial owners

---

2. PRODUCTS & SERVICES RISK ASSESSMENT

Bitcoin (BTC) Trading & Custody

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Most liquid cryptocurrency, widely used for legitimate purposes but also ML/TF
Impact	MEDIUM (2) - Pseudo-anonymous, blockchain

	traceable, industry-standard asset
Overall Risk Score	4 (MEDIUM)

Controls:

- Blockchain analytics on all BTC transactions (AMLBot)
- Sanctions screening of wallet addresses
- Travel Rule compliance for VASP-to-VASP transfers (from 31 March 2026)
- Enhanced screening for mixer/tumbler interactions
- Transaction monitoring for structuring patterns

Ethereum (ETH) & ERC-20 Tokens

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Smart contract functionality increases complexity, token variety
Impact	MEDIUM (2) - Traceable via blockchain, established ecosystem
Overall Risk Score	4 (MEDIUM)

Controls:

- Token-specific risk assessment (case-by-case for new tokens)
- Smart contract interaction monitoring
- Blockchain analytics covering ERC-20 transfers
- DeFi protocol interaction monitoring
- Travel Rule compliance for all VASP transfers

Stablecoins (USDT, USDC, DAI, etc.)

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Preferred for remittances and arbitrage, potential for sanctions evasion
Impact	MEDIUM (2) - Fiat-pegged, transparent on-chain
Overall Risk Score	4 (MEDIUM)

Controls:

- Enhanced monitoring for cross-border stablecoin transfers
- Issuer sanctions screening (Tether, Circle, etc.)
- Remittance corridor monitoring (Australia-Philippines)
- Travel Rule compliance critical for stablecoin VASP transfers
- Blockchain analytics for wallet risk assessment

Tron (TRX) & TRC-20 Tokens

Risk Factor	Assessment
Likelihood	MEDIUM-HIGH (2.5) - Popular in Asia, lower transaction costs attract certain use cases
Impact	MEDIUM (2) - Blockchain traceable but different ecosystem
Overall Risk Score	5 (MEDIUM)

Controls:

- Blockchain analytics specific to Tron network
- Enhanced monitoring for USDT-TRC20 (widely used in remittances)
- Cross-chain transaction pattern analysis
- Travel Rule compliance for Tron-based VASP transfers

P2P Arbitrage Operations

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Legitimate business model but requires careful monitoring
Impact	MEDIUM (2) - Higher transaction volumes, cross-platform activity
Overall Risk Score	4 (MEDIUM)

Controls:

- Enhanced due diligence on arbitrage traders
- Source of funds verification for trading capital
- Monitoring for wash trading or market manipulation patterns
- Cross-platform transaction correlation
- Regular review of P2P trading strategies

---

3. DELIVERY CHANNELS & TECHNOLOGY RISK ASSESSMENT

Digital Platform (Non-Face-to-Face Onboarding)

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Remote onboarding inherently higher risk than face-to-face
Impact	MEDIUM (2) - Identity fraud risk, synthetic identity
Overall Risk Score	4 (MEDIUM)

Controls:

- Electronic ID verification via KYC-AID and Sumsub
- Liveness detection to prevent photo/video spoofing
- Device fingerprinting and IP analysis
- Multi-factor authentication (MFA) mandatory
- Behavioral biometrics monitoring
- 55+ age fraud prevention calls (Section 32.9)
- Document verification (authenticity checks)

Instant Payment Integration (Monoova OSKO/PayID)

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Real-time payments reduce friction but increase fraud risk
Impact	MEDIUM (2) - Faster fund movement, potential for fraud losses
Overall Risk Score	4 (MEDIUM)

Controls:

- Real-time transaction monitoring
- Duplicate payment detection (address systematic NPP integration issues)
- Payment velocity limits per customer risk tier
- Bank account name matching
- First deposit hold period (24-48 hours for new customers)
- Withdrawal limits for new customers (graduated increase over 30 days)

Blockchain-Based Transfers

Risk Factor	Assessment
Likelihood	MEDIUM (2) - Pseudo-anonymous, cross-border capability
Impact	MEDIUM (2) - Traceable but requires specialized analytics
Overall Risk Score	4 (MEDIUM)

Controls:

- AMLBot blockchain analytics on all cryptocurrency deposits and withdrawals
- Wallet address risk scoring via AMLBot
- Real-time screening for sanctioned addresses (OFAC, DFAT, UN)
- Blacklisted exchange detection (non-compliant or high-risk exchanges)
- Clustering analysis to identify related addresses
- Sanctions screening of wallet addresses

- Travel Rule implementation (from 31 March 2026)
- Enhanced monitoring for mixer/tumbler interactions flagged by AMLBot
- Cross-chain transaction tracking
- AMLBot alerts for darknet marketplace connections, ransomware, and theft associations

---

4. GEOGRAPHIC & JURISDICTIONAL RISK ASSESSMENT

Australia (Primary Operations)

Risk Factor	Assessment
Likelihood	LOW (1) - Robust AML/CTF framework, AUSTRAC oversight, FATF compliant
Impact	LOW (1) - Strong rule of law, effective enforcement
Overall Risk Score	1 (LOW)

Controls:

- Full compliance with AML/CTF Act and Rules
- AUSTRAC reporting (TTR, IVTS, SMR)
- Regular engagement with AUSTRAC
- Participation in AUSTRAC industry consultations
- Domestic sanctions screening (DFAT Consolidated List)

Australia-Philippines Remittance Corridor

Risk Factor	Assessment
Likelihood	LOW-MEDIUM (1.5) - Philippines is FATF

	compliant, established remittance market
Impact	MEDIUM (2) - Cross-border transfers, larger amounts
Overall Risk Score	3 (LOW-MEDIUM)

Controls:

- Enhanced due diligence for remittance customers
- Source of funds verification
- Beneficiary identification for large transfers (>$5,000)
- Travel Rule compliance mandatory (from 31 March 2026)
- Monitoring for structuring (multiple transfers to same beneficiary)
- Philippines sanctions screening
- Counterparty VASP due diligence (UnionBank, Coins.ph, etc.)

FATF-Compliant Jurisdictions (UK, EU, US, Singapore, etc.)

Risk Factor	Assessment
Likelihood	LOW (1) - Strong AML/CTF frameworks, regulatory oversight
Impact	LOW (1) - Transparent systems, cooperative enforcement
Overall Risk Score	1 (LOW)

Controls:

- Standard transaction monitoring
- Travel Rule compliance
- Sanctions screening (all applicable lists)
- VASP counterparty verification

High-Risk Jurisdictions (FATF Grey/Black Lists)

Risk Factor	Assessment
Likelihood	HIGH (3) - Weak AML/CTF frameworks, corruption, sanctions
Impact	HIGH (3) - Severe regulatory and reputational risk
Overall Risk Score	9 (HIGH) - RESTRICTED/PROHIBITED

Controls:

- TRANSACTIONS GENERALLY PROHIBITED to/from sanctioned jurisdictions
- Enhanced due diligence if customer has connection to high-risk jurisdiction
- Immediate escalation to AML/CTF CO
- Senior management approval required
- Likely SMR filing required
- Travel Rule enhanced scrutiny
- Consider refusing service

Countries of Concern:

- OFAC Sanctioned: North Korea, Iran, Syria, Cuba, Russia (certain sectors), Venezuela (certain sectors)
- FATF High-Risk: (refer to current FATF public statements)
- DFAT Autonomous Sanctions: (refer to current DFAT Consolidated List)

---

5. PROLIFERATION FINANCING RISK ASSESSMENT

CoinPort's Overall PF Risk Profile

Risk Factor	Assessment
Likelihood	LOW-MEDIUM (1.5) - Diverse customer base including corporate entities increases complexity
Impact	MEDIUM (2) - Regulatory consequences if PF occurs
Overall Risk Score	3 (LOW-MEDIUM)

Rationale:

- CoinPort services individuals, companies, trusts, and institutional clients (Section 30.2)
- Corporate customers could potentially be front companies for proliferation networks (requires enhanced screening)
- No trade finance or dual-use goods transactions (reduces risk)
- No business in jurisdictions of PF concern (North Korea, Iran)

- Comprehensive sanctions screening includes PF-related designations
- Enhanced due diligence for corporate structures that could obscure ownership

Controls:

- Proliferation financing sanctions screening (UN, OFAC, DFAT) for all customer types
- Enhanced beneficial ownership verification for corporate customers
- Screening of corporate customers against WMD-related industry lists
- Transaction monitoring for unusual patterns indicating PF
- Staff training on PF red flags including corporate front company indicators
- Enhanced scrutiny for customers with connections to WMD-related industries or dual-use goods
- Immediate escalation if PF indicators identified
- Additional screening for complex corporate structures that could be used for sanctions evasion

---

6. ADVERSE EVENT TRIGGERS FOR RISK ASSESSMENT REVIEW

CoinPort will conduct immediate risk assessment review following any of these events:

Regulatory Events:

- AUSTRAC enforcement action or warning
- Regulatory examination findings

- Changes to AML/CTF Act or Rules
- New FATF recommendations or guidance
- Sanctions list updates affecting CoinPort customers

Operational Events:

- Significant compliance breach (e.g., missed SMR, failed Travel Rule transmission)
- Fraud incident affecting customers (>$10,000 loss)
- Data breach or cybersecurity incident
- Employee misconduct related to AML/CTF
- Systematic control failure (e.g., duplicate payment issue)

Business Changes:

- Introduction of new cryptocurrency assets
- Entry into new geographic markets
- New payment methods or banking partners
- Significant increase in customer base (>50% growth in 3 months)
- Change in customer demographics or risk profile
- New product or service offerings

External Events:

- Major ML/TF incident in virtual asset sector
- New ML/TF typology identified by AUSTRAC
- Sanctions developments (new designations)
- Adverse media coverage of CoinPort
- VASP counterparty enforcement action

7. RISK MITIGATION STRATEGIES SUMMARY

Risk Category	Current Risk Level	Target Risk Level	Key Mitigating Controls
Customer Risk	MEDIUM	MEDIUM	Comprehensive KYC across all entity types, beneficial ownership verification, PEP enhanced CDD, 55+ fraud screening, corporate structure analysis
Product Risk	MEDIUM	MEDIUM	AMLBot blockchain analytics, sanctions screening, Travel Rule from March 2026
Channel Risk	MEDIUM	LOW-MEDIUM	Electronic verification, liveness detection, instant payment monitoring, AMLBot wallet screening
Geographic Risk	LOW	LOW	Australia-focused, limited cross-border, VASP counterparty due diligence
Proliferation Financing	LOW-MEDIUM	LOW	Enhanced sanctions screening via AMLBot, beneficial ownership verification for corporates, no trade finance

8. CONTINUOUS IMPROVEMENT INITIATIVES

Q1 2026:

- ☑ Travel Rule implementation with Sumsub and Notabene (deadline: 31 March 2026)
- ☑ Unified AML/CTF Program adoption (replacing Part A/Part B structure)
- ☑ VASP counterparty due diligence procedures documented
- ☑ AMLBot blockchain analytics integration
- ⏳ Initial post-implementation review scheduled (February 2026) - One month check-in on Version 3.0 effectiveness, Travel Rule readiness, new customer type procedures

Q2 2026:

- Blockchain analytics tool effectiveness review (AMLBot performance assessment)
- Transaction monitoring false positive rate reduction project
- Enhanced PEP screening automation
- Staff training on Travel Rule and 2026 reforms
- Review findings from February 2026 initial review and implement any required adjustments

Q3 2026:

- Risk assessment methodology review

- Customer risk rating accuracy assessment
- Sanctions screening database consolidation
- Travel Rule system testing and optimization post go-live

Q4 2026:

- Program content review (prepare for January 2027 annual review)
- Gather metrics for annual independent audit
- Lessons learned from first year of outcomes-based regime
- 2027 risk assessment planning

2027 Ongoing:

- Annual independent review each January (next: January 2027)
- Quarterly internal reviews continue
- Continuous improvement based on operational experience and regulatory guidance

---

9. KEY RISK INDICATORS (KRIs) - MONITORING DASHBOARD

CoinPort tracks the following KRIs monthly:

KRI	Target	Red Flag Threshold
SMR submission rate	>0 when suspicious activity detected	Failure to submit within required timeframe
TTR submission rate	100% within 10	<95% compliance

(>$10k)	business days	
False positive rate (transaction monitoring)	<30%	>50%
Customer KYC refresh completion	>95% on schedule	<90%
Staff training completion	100% annually	<100%
Travel Rule message success rate	>95% (from March 2026)	<90%
Sanctions screening coverage	100%	<100%
AML/CTF CO escalations responded	100% within 24 hours	<100%

Risk Assessment Matrix Owner: AML/CTF Compliance Officer
Last Updated: 5 January 2026
Next Scheduled Review: 5 April 2026 (Quarterly)
Board Approval Date: 5 January 2026

APPENDIX 4 – VASP COUNTERPARTY DUE DILIGENCE (CDD) QUESTIONNAIRE

PURPOSE AND SCOPE

This questionnaire must be completed by any counterparty Virtual Asset Service Provider (VASP) before CoinPort Exchange will facilitate Travel Rule data exchange or process VASP-to-VASP cryptocurrency transfers. This procedure implements Section 25.4 (VASP Counterparty Due Diligence - Mandatory Requirement).

Standard: GDF/Wolfsberg-Aligned VASP Scorecard
Responsible Officer: Nicanor Nuqui, AML/CTF Compliance Officer
Frequency: Initial onboarding + Annual refresh for Medium/High risk VASPs
Legal Basis: AML/CTF Act Section 25.4, Travel Rule (effective 31 March 2026)

VASP COUNTERPARTY DUE DILIGENCE QUESTIONNAIRE

INSTRUCTIONS FOR COUNTERPARTY VASP:
Please complete all sections truthfully and provide supporting documentation where requested. CoinPort will use these responses to assess our ability to exchange Travel Rule information with your organization. Incomplete responses may result in transaction delays or rejection.

Date Completed: _____
Completed By: _____
Position/Title: _____

Section	Question for Counterparty VASP	Response	Supporting Documents	Key Requirement
1. IDENTITY & REGISTRATION				
1.1	What is your full legal name?			CRITICAL: Must match "Known VASP" directories (Notabene, TRISA, VASP Directory)
1.2	What are your trading names or brand names (if different)?			Verifies public-facing identity
1.3	What is your registered business address?		Certificate of Incorporation or Registration	CRITICAL: Cannot be PO Box or Virtual Office for VASP registration
1.4	What is your			CRITICAL: Check

	country of incorporation?			against FATF high-risk/grey-listed regions, sanctioned jurisdictions
1.5	Are you licensed/registered as a VASP (or equivalent: DCE, MSB, PSP)?	☐ Yes ☐ No		CRITICAL: "No" = Automatic Block from 31 March 2026
1.6	If YES to 1.5: What is your regulator name and license/registration number?	Regulator: _____ License #: _____	Copy of License or link to public register	Verify via AUSTRAC VASP Register, FinCEN MSB Registry, FCA Register, etc.
1.7	When was your VASP license/registration issued or last			KEY: Expired licenses = Medium/High Risk

	renewed?			
1.8	Are your customer assets segregated from corporate funds (on-chain or in trust)?	☐ Yes ☐ No ☐ N/A		Risk Factor: Mitigates counterparty insolvency risk
1.9	What is your website URL?			Cross-reference with public VASP directories
1.10	What is your primary email domain for compliance communications?			Verify domain ownership matches legal entity
2. AML/CTF PROGRAM				
2.1	Do you have a written, Board-	☐ Yes ☐ No	Table of Contents or Executive	KEY: Confirms structural compliance

	approved AML/CTF Program?		Summary	e
2.2	When was your AML/CTF Program last approved by your Board or senior managem ent?			Programs > 2 years old without review = Red Flag
2.3	Does your AML/CTF Program undergo independe nt audits or reviews?	☐ Yes ☐ No		KEY: Proves program effectivene ss
2.4	If YES to 2.3: When was your last independe nt AML/CTF audit?		Summary of findings (if available)	Audits >18 months old = Medium Risk
2.5	Has your entity been subject to	☐ Yes ☐ No	Details if Yes	Risk Factor: If Yes: High

	any regulatory fines, sanctions, or enforcement actions in the last 24 months?			Risk, Manual Review required
2.6	Do you have a designated AML/CTF Compliance Officer?	☐ Yes ☐ No	Name and contact details	Required for escalations
3. KYC & CUSTOMER DUE DILIGENCE				
3.1	Do you perform KYC verification on ALL customers before they can transact?	☐ Yes ☐ No		KEY: Ensures clean ecosystem
3.2	What KYC verification methods	☐ Electronic verification ☐	Name of KYC provider if	Electronic + Document

	do you use?	Document verification ☐ In-person ☐ Third-party KYC provider	applicable	= Standard
3.3	What is your policy for identifying Politically Exposed Persons (PEPs)?	☐ Screen all customers ☐ Screen high-risk only ☐ No PEP screening		KEY: Required for PEP monitoring
3.4	Do you apply Enhanced Due Diligence (EDD) for high-risk customers?	☐ Yes ☐ No		Standard risk-based requirement
3.5	What types of customers do you service?	☐ Individual retail ☐ Corporate/ Business ☐ Institutional ☐ Other: _____		Higher corporate mix = Higher complexity
3.6	How do you	☐ Signature		CRITICAL: AI

	verify ownership for self-hosted (unhosted) wallet transfers?	verification ☐ Test transaction ☐ Customer declaration only ☐ No verification		igns with AUSTRAC $10k threshold rules
4. SANCTIONS & FINANCIAL CRIME SCREENING				
4.1	Do you screen customers and transactions against sanctions lists?	☐ Yes ☐ No		KEY: Mandatory for AML/CTF compliance
4.2	Which sanctions lists do you screen against?	☐ UN Security Council ☐ OFAC (USA) ☐ DFAT (Australia) ☐ EU ☐ UK HMT ☐		KEY: Must include minimum UN + local jurisdiction

		Other: _____		
4.3	Do you screen sanctions in real-time (before transaction processing)?	☐ Yes ☐ No		CRITICAL: Batch screening creates violation window
4.4	Do you have specific controls to detect Proliferation Financing (WMD-related)?	☐ Yes ☐ No	Brief description	KEY: New 2026 legal obligation
4.5	Do you screen for dual-use goods transactions or PF-linked shell companies?	☐ Yes ☐ No ☐ N/A		Advanced: Higher-tier compliance
4.6	What is your	☐ Immediate		Immediate block =

	process when a sanctions hit is identified?	transaction block ☐ Manual review first ☐ Customer notification ☐ Other: _____		Best practice
5. TRAVEL RULE & TECHNICAL CAPABILITIES				
5.1	Which Travel Rule messaging protocol(s) do you use?	☐ Notabene ☐ TRP ☐ TRISA ☐ Sygna Bridge ☐ Other: _____ ☐ None yet (planned date: ___)		KEY: Confirms interoperability
5.2	Can you securely receive, store, and transmit PII per GDPR/privacy laws?	☐ Yes ☐ No	Privacy Policy or Data Protection summary	CRITICAL: Protects from data leak liability
5.3	Do you	☐ Yes ☐ No		Advanced:

	support “Check-First” or “First-Share” protocols for Travel Rule exchanges ?			Highest standard for data privacy
5.4	Do you have documented procedures for handling Travel Rule failures?	☐ Yes ☐ No		Demonstrates operational maturity
5.5	What is your average Travel Rule response time?	☐ <1 hour ☐ 1-4 hours ☐ 4-24 hours ☐ >24 hours		Response time affects customer experience
5.6	Do you have 24/7 Travel Rule operations or business	☐ 24/7 ☐ Business hours only	Business hours if applicable	24/7 = Better for international customers

	hours only?			
6. TRANSACTION MONITORING & BLOCKCHAIN ANALYTICS				
6.1	Which blockchain analytics tool(s) do you use?	☐ Chainalysis ☐ Elliptic ☐ TRM Labs ☐CipherTrace ☐ AMLBot ☐ Other: _____ ☐ None		KEY: “None” = High Risk. CoinPort uses AMLBot
6.2	Do you screen cryptocurrency wallet addresses before processing deposits/withdrawals?	☐ Yes ☐ No		Standard requirement
6.3	What is your policy for high-risk wallet interactions	☐ Automatic block ☐ Enhanced review		KEY: Aligns risk appetite

	(mixers, tumblers, darknet)?	☐ Customer contact ☐ Process normally		
6.4	Do you monitor for transaction structuring or unusual patterns?	☐ Yes ☐ No		Required for SMR
6.5	Have you filed Suspicious Activity Reports (SARs/SMRs) in the past 12 months?	☐ Yes ☐ No ☐ Prefer not to disclose		Demonstrates active monitoring
7. ADDITIONAL INFORMATION				
7.1	What is your estimated monthly transaction volume in USD equivalent?	☐ <$1M ☐ $1M-$10M ☐ $10M-$100M ☐ >$100M		Risk scales with volume
7.2	What			Cross-

	geographic markets do you primarily serve?			reference with high-risk jurisdictions
7.3	Do you have any pending regulatory examinations or investigations?	☐ Yes ☐ No ☐ Prefer not to disclose		If Yes: High Risk pending resolution
7.4	Are you willing to provide quarterly compliance attestations to CoinPort?	☐ Yes ☐ No		Demonstrates partnership commitment

INTERNAL VASP RISK SCORING KEY (AML/CTF CO USE ONLY)

Instructions for AML/CTF Compliance Officer (Nicanor Nuqui): After receiving completed questionnaire, apply the following logic gates to assign a Risk Rating. Document rationale for risk classification.

AUTOMATIC DECISION RULES:

Risk Rating	Trigger Conditions	Action Required
CRITICAL (REJECT)	• VASP is unlicensed/unregistered (Q1.5 = No) • Operating from sanctioned jurisdiction (Q1.4) • VASP appears on sanctions lists • Recent major enforcement action (Q2.5 = Yes, severe) • Cannot securely handle PII (Q5.2 = No)	ACTION: Cease all transaction attempts. Add to "Blocked VASPs" list. Decline customer transactions to this VASP. Document decision and inform customer (without tipping off).
HIGH (MANUAL REVIEW)	• No independent AML/CTF audit (Q2.3 = No) • No Proliferation Financing controls (Q4.4 = No) • No blockchain analytics tool (Q6.1 = None)	ACTION: AML/CTF CO must manually approve EACH transaction over $5,000. Enhanced monitoring required. Consider limiting transaction

	• No sanctions screening (Q4.1 = No) • Recent regulatory fine (Q2.5 = Yes)	amounts. Quarterly review mandatory.
MEDIUM (MONITORED)	• Uses different/incompatible Travel Rule protocol (Q5.1) • Incomplete sanctions screening (Q4.2 missing key lists) • No real-time sanctions screening (Q4.3 = No) • Slow Travel Rule response time (Q5.5 >24 hours) • AML/CTF program >2 years old without review • No PEP screening (Q3.3 = No PEP screening)	ACTION: Apply enhanced monitoring. May use "Sunrise Solution" (manual data exchange). Transaction cap: $10,000 per transfer. Semi-annual CDD refresh. Document all transactions.
LOW (TRUSTED)	• Licensed VASP with verified registration (Q1.5 = Yes, Q1.6 verified) • Uses compatible Travel Rule protocol (Q5.1 = Notabene/TRP/TRISA) • Independent audit within 18 months (Q2.4) • Comprehensive sanctions screening	ACTION: Add to "Approved VASP List" for automated Travel Rule clearing. Standard transaction monitoring applies. Annual CDD refresh. Expedited transaction

	(Q4.2 all major lists) • Uses tier-1 blockchain analytics (Q6.1 = Chainalysis/Elliptic/TRM) • No enforcement history (Q2.5 = No)	processing.

VASP COUNTERPARTY APPROVAL WORKFLOW

Step 1: Pre-Questionnaire Screening (5 minutes)

- Check Notabene VASP Directory for existing verification
- Check AUSTRAC Public VASP Register (if Australian)
- Check FinCEN MSB Registry (if US-based)
- Google search for recent enforcement actions or negative media
- If verified in trusted directory: May apply Simplified Due Diligence (skip to Step 4)

Step 2: Send Questionnaire (Same day)

- Email questionnaire to counterparty VASP compliance officer
- Request response within 10 business days
- Set reminder for follow-up if no response

Step 3: Review & Score (2-3 business days after receipt)

- Verify responses against supporting documents
- Cross-check license numbers with regulator public databases

- Apply Risk Scoring Key (above) to assign rating
- Document rationale for risk classification
- If CRITICAL rating: Escalate to Board immediately

Step 4: Management Approval

- LOW Risk: AML/CTF CO approval (document in file)
- MEDIUM Risk: AML/CTF CO + Senior Management approval
- HIGH Risk: Board approval required (present at next Board meeting)

Step 5: Add to VASP Registry

- Enter VASP details into "Approved VASP List" or "Restricted VASP List"
- Configure Travel Rule system with counterparty details
- Set transaction limits based on risk rating
- Schedule next review date (Annual for Medium/High; 2 years for Low)

Step 6: Ongoing Monitoring

- Quarterly: Check for sanctions list updates affecting counterparty
- Quarterly: Monitor for negative media or enforcement actions
- Annually (Medium/High) or Biannually (Low): Re-send questionnaire for refresh
- Ad hoc: Investigate if Travel Rule failures exceed 10% with this counterparty

INTEGRATION NOTES FOR AML/CTF COMPLIANCE OFFICER

Directory Check Before Questionnaire:
Before sending this questionnaire, always check:

1. Notabene VASP Directory - Pre-verified VASPs may qualify for simplified DD
2. AUSTRAC Public VASP Register - Australian VASPs (from 31 March 2026)
3. FinCEN MSB Registry - US-based Money Services Businesses
4. FCA Register - UK Financial Conduct Authority registered firms
5. MAS Licensing Register - Singapore Monetary Authority VASPs

If VASP is already "Verified" in a trusted directory operated by a FATF-compliant regulator, you may:

- Skip Questions 1.5-1.7 (already verified)
- Reduce review frequency to 24 months (instead of 12 months)
- Apply LOW risk rating by default (unless other red flags present)

Annual Refresh Requirements:
This questionnaire must be re-sent to:

- HIGH risk VASPs: Every 12 months + any time there's an adverse event
- MEDIUM risk VASPs: Every 12 months
- LOW risk VASPs: Every 24 months

Red Flags Requiring Immediate Re-Assessment:

- Counterparty VASP receives regulatory enforcement action
- Counterparty VASP changes ownership or senior management
- Pattern of Travel Rule failures (>10% failure rate over 30 days)
- Counterparty appears in adverse media for AML/CTF failures
- Counterparty's license expires or is suspended
- Counterparty jurisdiction added to FATF grey/black list

Travel Rule Failure Documentation:
If a counterparty VASP repeatedly fails to respond to Travel Rule messages:

1. Document 3+ failed attempts over 24-hour period
2. Escalate to MEDIUM risk (if not already HIGH/CRITICAL)
3. Notify customer of delay (without disclosing VASP compliance issues)
4. Consider alternative routing if customer has accounts at other VASPs
5. After 5 consecutive failures: Suspend transactions to this VASP pending review

Sanctions Screening of Counterparty VASPs:
Before approving any VASP:

- Screen VASP entity name against DFAT Consolidated List
- Screen VASP entity name against OFAC SDN List
- Screen beneficial owners (if known) against sanctions lists

- Screen VASP's country of operation against sanctioned jurisdictions
- If sanctions hit: Automatic CRITICAL rating, report to DFAT/AUSTRAC

DOCUMENTATION & RECORD KEEPING

Required Records (7-year retention per Section 20):

- Completed questionnaire with all supporting documents
- Risk scoring rationale and decision memo
- Management/Board approval documentation
- Verification checks (license lookups, directory searches)
- All Travel Rule messages exchanged with this VASP
- Annual refresh questionnaires and risk re-assessments
- Any adverse events or Travel Rule failures
- Communications with counterparty regarding compliance issues

File Location: `Compliance/VASP-Counterparty-DD/[VASP Name]/`

Naming Convention: `[VASP-Name]_CDD-Questionnaire_[Date]_v[Version].pdf`

APPENDIX 4 VERSION CONTROL

Version	Date	Changes
1.0	5 January 2026	Initial questionnaire aligned with Section 25.4 requirements and GDF/Wolfsberg VASP standards

Next Review: 5 January 2027 or upon regulatory guidance updates

---

Appendix Owner: AML/CTF Compliance Officer
Approved By: Board of Directors, 5 January 2026

PROGRAM APPROVAL AND SIGNATURES

Issued by the Board of Directors of CoinPort Pty Ltd

Program Effective Date: 5 January 2026

BOARD APPROVAL

This AML/CTF Program Version 3.0 was reviewed and approved by the Board of Directors of CoinPort Pty Ltd on 5 January 2026.

Board Chairperson / CEO:

Kent Kingsley
Chief Executive Officer
Date: _____

Director / CTO/CFO:

Peter Cooney
Chief Technology Officer / Chief Financial Officer
Date: _____

AML/CTF COMPLIANCE OFFICER ACKNOWLEDGEMENT

I acknowledge my appointment as AML/CTF Compliance Officer and accept responsibility for implementing and overseeing CoinPort's obligations under this Program, the AML/CTF Act, and the AML/CTF Rules.

AML/CTF Compliance Officer:

_____

Nicanor Nuqui
AML/CTF Compliance Officer
Date: _____

PROGRAM DISTRIBUTION

This Program has been distributed to:

- All Board Members
- All CoinPort Employees
- Third-Party Service Providers (KYC-AID, Sumsub, Notabene, AMLBot)
- Legal Counsel
- External Auditor
- Compliance Consultant

DOCUMENT CONTROL

Version	Date	Author	Changes Summary
1.0	6 June 2021	[Name]	Original Part A and Part B prepared
2.0	1 July 2024	[Name]	Edits for fraud prevention (55+ screening)
3.0	5 January 2026	[Name]	Unified program for 2026 AML/CTF reforms; Travel Rule implementation; DCE→VASP transition; Risk-based approach adoption; Proliferation financing added; Section 25.2 updated with current reporting obligations

Next Scheduled Review: February 2026 (initial post-implementation), then January 2027 (annual)
Document Location: CoinPort secure document management system
Access Level: Board, Management, AML/CTF CO, AUSTRAC (upon request)

END OF DOCUMENT

CoinPort Pty Ltd
AUSTRAC Registration Number: 100633359
Independent Remittance Dealer: IND100633359-001
Legal Entity: CoinPort PTY LTD