Anti-Money Laundering and Counter-Terrorism Financing Policy

Coin Harbour Pty Ltd

Company:	Coin Harbour Pty Ltd
ACN:	624 879 223
Date Updated:	6-June-2021

TABLE OF CONTENTS

VERSION CONTROL

Version Number	Date Updated	Notes
1	6-Jun-2021	Original document prepared and finalised.

INTRODUCTION

1. OVERVIEW

1.1 The *Anti-Money Laundering (**"AML"**) and Counter-Terrorism Financing (**"CTF"**) Act* 2006 (**"AML/CTF Act"**) received Royal Assent on 12 December 2006. The broad purpose of the AML/CTF Act 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 Money laundering involves the injection of funds generated from illegal activities into the legitimate financial system in order to hide or disguise the criminal source of those funds. Terrorism Financing is the use of money, which may or may not be generated from criminal activity, for financing terrorist activities. Recently, Digital Currency Exchange Providers have been used by criminals to launder the proceeds of crime and/or facilitate the financing of terrorism.

2. ABOUT THE AML/CTF ACT

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

2.2 Digital Currency Exchange Providers provide a designated service listed in the AML/CTF Act and are therefore reporting entities. These services are included in the AML/CTF Act because they are vulnerable to abuse by criminals for money laundering or terrorism financing purposes.

2.3 The AML/CTF Act adopts a risk-based approach. This approach means that the reporting entity will decide how best to identify, mitigate and manage the risk of money laundering and terrorism financing through its business. Reporting entities will therefore need to undertake a comprehensive assessment of these risks relative to their businesses. Reporting entities will need to be able to demonstrate to AUSTRAC that they have carried out such an assessment and have a documented program in place to identify, mitigate and manage the risk of their products or services being used to facilitate money laundering or terrorism financing.

3. SUMMARY OF GENERAL OBLIGATIONS

3.1 Reporting entities must:

(a) have and carry out prescribed procedures to verify a customer's identity before providing a designated service;

(b) adopt and maintain an AML/CTF program;

(c) have an AML/CTF Compliance Officer;

(d) enrol and register with AUSTRAC;

(e) report suspicious matters to AUSTRAC's Chief Executive Officer (**"CEO"**); and

(f) undertake ongoing customer due diligence.

4. DEFINITIONS

4.1 Words and phrases defined in the AML/CTF Act or Rules have the same meaning when used in Coin Harbour Pty Ltd's (**"Coin Harbour"**) AML/CTF Program (**"Program"**) unless otherwise specified.

4.2 **Australian Government Entity** means:

(a) the Commonwealth, a State or a Territory; or

(b) an agency or authority of:

(i) the Commonwealth; or

(ii) a State; or

(iii) a local governing body established by or under a law of the Commonwealth, a State or Territory, other than a body whose sole or principal function is to provide a particular service, such as the supply of electricity or water;

4.3 **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'.

4.4 **Beneficial Owner:**

(a) of a person who is a reporting entity, means an individual who owns or controls (directly or indirectly) the reporting entity;

(b) of a person who is a customer of a reporting entity, means an individual who ultimately owns or controls (directly or indirectly) the customer;

(c) in this definition, *control* includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies; and

(d) in this definition, *owns* means ownership (either directly or indirectly) of 25% or more of a person.

4.5 **Digital currency:**

(a) 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

(b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;

but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of this Act.

4.6 **Digital Currency Exchange Provider** means a person running a business that exchanges digital currency with money or vice versa.

4.7 **Digital Currency Exchange Register** means the register of Digital Currency Exchange Providers maintained by the AUSTRAC CEO for the purposes of Part 6A of the AML/CTF Act.

4.8 **Politically Exposed Persons** (**"PEP"**) means an individual:

(a) who holds a prominent public position or function in a government body or an international organisation, including:

(i) Head of State or head of a country or government; or

(ii) government minister or equivalent senior politician; or

(iii) senior government official; or

(iv) Judge of the High Court of Australia, the Federal Court of Australia or a Supreme Court of a State or Territory, or a Judge of a court of equivalent seniority in a foreign country or international organisation; or

(v) governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of Australia; or

(vi) senior foreign representative, ambassador, or high commissioner; or

(vii) high-ranking member of the armed forces; or

(viii) board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise or international organisation; and

(b) who is an immediate family member of a person referred to in paragraph 4.8(a), including:

(i) a spouse; or

(ii) a de facto partner; or

(iii) a child and a child's spouse or de facto partner; or

(iv) a parent; and

(c) who is a close associate of a person referred to in paragraph 4.8(b), which means any individual who is known (having regard to information that is public or readily available) to have:

(i) joint beneficial ownership of a legal entity or legal arrangement with a person referred to in paragraph 4.8(b); or

(ii) sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph 4.8(b).

(d) In this Program:

(i) *domestic politically exposed person* means a politically exposed person of an Australian government body;

(ii) *foreign politically exposed person* means a politically exposed person of a government body of a foreign country;

(iii) *international organisation politically exposed person* means a politically exposed person of an international organisation.

(e) In this definition *international organisation* means an organisation:

(i) established by formal political agreement by two or more countries and that agreement has the status of an international treaty; and

(ii) recognised in the law of the countries which are members of the organisation.

4.9 **Primary non-photographic identification document** means:

(a) a birth certificate or birth extract issued by a State or territory;

(b) a citizenship certificate issued by the Commonwealth;

(c) a citizenship certificate issued by a foreign government that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator;

(d) a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator; or

(e) a concession card, as defined from time to time in the Social Security Act 1991, or an equivalent term which expresses the same concept in relation to concession holders.

4.10 **Primary photographic identification document** means:

(a) a licence or permit issued under a law of a State or Territory or equivalent authority of a foreign country for the purpose of driving a vehicle that contains a photograph of the person in whose name the document is issued;

(b) a passport issued by the Commonwealth;

(c) a passport or a similar document issued for the purpose of international travel, that:

(i) contains a photograph and either:

(A) the signature of the person in whose name the document is issued; or

(B) any unique identifier of the person in whose name the document is issued;

(ii) is issued by a foreign government, the United Nations or an agency of the United Nations; and

(iii) if it is written in a language that is not understood by the person carrying out the verification - is accompanied by an English translation prepared by an accredited translator;

(d) a card issued under a law of a State or Territory for the purpose of proving the person's age which contains a photograph of the person in whose name the document is issued;

(e) a national identity card issued for the purpose of identification, that:

(i) contains a photograph and either:

(A) the signature of the person in whose name the document is issued; or

(B) any unique identifier of the person in whose name the document is issued;

(ii) is issued by a foreign government, the United Nations or an agency of the United Nations; and

(iii) if it is written in a language that is not understood by the person carrying out the verification - is accompanied by an English translation prepared by an accredited translator.

4.11 **Reasonable measures** means appropriate measures which are commensurate with the money laundering or terrorism financing risks.

4.12 **Registrable Digital Currency Exchange Service** means a designated service that:

(a) is covered by item 50A of table 1 in section 6 of the AML/CTF Act; and

(b) is not of a kind specified in the AML/CTF Rules.

4.13 **Secondary Identification Document** means:

(a) a notice that:

(i) was issued to an individual by the Commonwealth, a State or Territory within the preceding twelve months;

(ii) contains the name of the individual and his or her residential address; and

(iii) records the provision of financial benefits to the individual under a law of the Commonwealth, State or Territory (as the case may be);

(b) a notice that:

(i) was issued to an individual by the Australian Taxation Office within the preceding 12 months;

(ii) contains the name of the individual and his or her residential address; and

(iii) records a debt payable to or by the individual by or to (respectively) the Commonwealth under a Commonwealth law relating to taxation;

(c) a notice that:

(i) was issued to an individual by a local government body or utilities provider within the preceding three months;

(ii) contains the name of the individual and his or her residential address; and

(iii) records the provision of services by that local government body or utilities provider to that address or to that person.

(d) in relation to a person under the age of 18, a notice that:

(i) was issued to a person by a school principal within the preceding three months;

(ii) contains the name of the person and his or her residential address; and

(iii) records the period of time that the person attended at the school.

4.14 **Senior managing official** means an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer of a reporting entity or who has the capacity to affect significantly the financial standing of a customer of a reporting entity.

5. AML/CTF PROGRAM

5.1 Coin Harbour adopts Parts A and B of this Program for the purposes of the AML/CTF Act. On and from 6-June-2021, Coin Harbour must comply with this Program, as varied from time to time.

6. RECORDS RELATING TO COIN HARBOUR'S AML/CTF PROGRAM

6.1 The AML/CTF Compliance Officer will ensure that the following records are retained for Coin Harbour:

(a) this Program and each variation to the Program;

(b) Coin Harbour approval of Part A of this Program, and each variation to Part A of 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.

6.2 The records referred to in Section 6.1 of this Program will be retained:

(a) in the case of records relating to the adoption of this Program and each variation to the 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.

7. AUSTRAC ENROLMENT AND REGISTRATION

7.1 Digital Currency Exchange Providers are required to enrol **and** register with AUSTRAC. Enrolment and registration are separate legal requirements and both must be completed.

7.2 Enrolment

(a) The AML/CTF Compliance Officer must enrol Coin Harbour with AUSTRAC within twenty-eight (28) days of providing or commencing to provide a designated service.

(b) The AML/CTF Compliance Officer must keep Coin Harbour's enrolment details up to date and notify AUSTRAC within fourteen (14) days of any changes to Coin Harbour's details.

7.3 Registration

(a) The AML/CTF Compliance Officer must register Coin Harbour as a digital currency exchange provider with AUSTRAC prior to providing or commencing to provide a Registrable Digital Currency Exchange Service.

(b) A Registrable Digital Currency Exchange Service must not be provided if Coin Harbour has not registered with AUSTRAC. Failure to register may constitute the commission of a criminal offence.

(c) Upon registration, Coin Harbour will be a Digital Currency Exchange Provider registered on the Digital Currency Exchange Register.

7.4 Renewal of registration

(a) Coin Harbour must submit an application for renewal of registration within the ninety (90) day period ending on the day on which Coin Harbour's registration would otherwise cease (being three (3) years after the day on which registration took effect).

(b) An application for renewal must be made using the approved form obtained from Coin Harbour's AUSTRAC Online Account, and must contain all relevant information prescribed by that form, including a declaration that:

(i) Coin Harbour has complied with the requirements of section 76P of the AML/CTF Act, where applicable; and

(ii) Coin Harbour's enrolment and registration details as they appear on both the Reporting Entities Roll and the Digital Currency Exchange Register are current and correct.

8. AML/CTF COMPLIANCE REPORTING

8.1 The AML/CTF Compliance Officer must submit, on behalf of Coin Harbour, an AML/CTF Compliance Report to AUSTRAC within three (3) months of the end of each Reporting Period (**"Reporting Period"**), or otherwise as specified by AUSTRAC.

8.2 The AML/CTF Compliance Report must cover each of Coin Harbour's compliance with the AML/CTF Act and Rules during the Reporting Period and take the form to be specified by AUSTRAC (if any).

9. PENALITIES

9.1 Failure to comply with the obligations under the AML/CTF Act may result in civil or criminal penalties.

9.2 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.

9.3 The penalties for criminal offences include imprisonment for up to 10 years and/or fines up to $1.7 million.

PART A – GENERAL

10. INTRODUCTION

10.1 Part A of this Program is designed to identify, mitigate and manage the risk which Coin Harbour may reasonably face that the provision of its designated services at or through a permanent establishment of that entity in Australia might involve or facilitate money laundering or terrorism financing. Additionally, Part A of this Program helps Coin Harbour's staff to understand the nature and purpose of the business relationship with its customer types, including, as appropriate, the collection of information relevant to that understanding.

11. ANALYSIS OF DESIGNATED SERVICES AND MONEY LAUNDERING OR TERRORISM FINANCING RISK

11.1 In determining and putting in place appropriate risk-based systems and controls to identify, mitigate and manage money laundering or terrorism financing risks in Part A of this Program, Coin Harbour has had regard to the following factors, the:

(a) nature, size and complexity of its business; and

(b) type of money laundering or terrorism financing risk that it might reasonably face.

11.2 Coin Harbour has also considered the following factors when identifying [insert defined Coin Harbour's exposure to money laundering or terrorism financing, the:

(a) customer types, including any politically exposed persons;

Coin Harbour will primarily deal with customers as specified in Section 25.2 of this Program;

(b) types of designated services provided;

Coin Harbour only deals in the following digital currencies:

(i) Bitcoin (BTC); and the various Bitcoin forks, such as Dash

(ii) Ether (ETH) and the various Ethereum blockchain tokens

(iii) Ethereum Classic (ETC) and various tokens on other Ethereum blockchain forks such as the Binance blockchain

(iv) Various tokens on the Tron blockchain

(v) Various tokens on the Monero blockchain

(vi) Various tokens on the Ripple blockchain

(c) Coin Harbour undertakes due diligence on the supply sources of the purchased digital currencies to ensure they are trusted and reliable. Coin Harbour will ensure it has a contractual agreement in place between [insert define company name name] and digital currency supply sources prior to providing customers with designated services.

(d) Coin Harbour offers the following services to customers as specified in Section 25.2 of this Program:

(i) Buying digital currency;

(ii) Selling digital currency;

(iii) Exchanging digital currency;

(iv) Holding digital currency (on trust or as custodian); and

(v) Participating in digital currency Initial Offerings

(e) methods by which those services are delivered; and

Coin Harbour will operate an electronic platform for recording, processing and settling electronic transactions requested by customers. All customers will be on boarded via the Coin Harbour website;

(f) jurisdictions in which those services are delivered;

Coin Harbour has identified 1 different customer types with whom Coin Harbour may transact, as specified in Section 25.2 of this Program. The jurisdictions that Coin Harbour intends to deal with are:

(i) Individuals

(g) Coin Harbour does not accept or provide physical cash to its customers in the course of providing its digital currency exchange services.

(h) Criminal threat environment and possible vulnerabilities of the Coin Harbour.

11.3 When identifying Coin Harbour's exposure to money laundering and terrorism financing, Coin Harbour:

(a) identifies significant changes in money laundering or terrorism financing risk;

(b) recognises such changes in money laundering or terrorism financing risk for the purposes of the requirements of this Program; and

(c) identifies, mitigates and manages any money laundering and terrorism financing risk posed by:

(i) all new designated services prior to introducing them to the market;

(ii) all new methods of designated service delivery prior to adopting them;

(iii) all new or developing technologies used for the provision of a designated service prior to adopting them; and

(iv) changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers.

11.4 Where Coin Harbour notices that any of the following significant changes to the customer's business have taken place, it must obtain further details in writing from the client to satisfy themselves that the client does not present an unacceptable risk. Significant changes can be identified as one of the following:

(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.

11.5 Coin Harbour provides the following designated services:

(a) Item 50A of section 6 of the AML/CTF Act - exchanging digital currency for money (whether Australian or not) or exchanging money (whether Australian or not) for digital currency, where the exchange is provided in the course of carrying on a digital currency exchange business.

11.6 Prior to a new designated service being introduced to the market by Coin Harbour, the AML/CTF Compliance Officer will assess it to determine whether it involves the provision of a designated service. Where it is determined that a new service involves the provision of a designated service, the AML/CTF Compliance Officer will assess the money laundering or terrorism financing risk involved in the provision of the designated service.

11.7 An assessment of the AML/CTF risk(s) posed to the Compliance Officer must also be conducted for all new:

(a) methods of designated service delivery prior to adopting them (for example, using a non-face-to-face method);

(b) or developing technologies used for the provision of a designated service prior to adopting them; and

(c) changes arising in the nature of the business relationship, control structure or beneficial ownership of Coin Harbour's customers.

11.8 The Board of Directors' approval must be received before a new designated service is introduced to the market by Coin Harbour. The Board of Directors must be given a copy of the risk assessment conducted under Section 11.7 of this Program, before the approval is granted.

11.9 Coin Harbour's Risk Assessment and Management Matrix which forms part of this Program takes into account:

(a) the nature, size and complexity of the business; and

(b) the type of money laundering or terrorism financing risk that might be reasonably faced by Coin Harbour.

11.10 Coin Harbour's Risk Assessment and Management Matrix should be read in conjunction with this Program and identifies:

(a) The types of designated services provided by Coin Harbour;

(b) The methods of delivery of Coin Harbour's services; and

(c) The foreign jurisdictions which Coin Harbour deals with (if applicable).

12. APPLICATION OF PART A

12.1 Part A of this Program applies to Coin Harbour in relation to all areas of its business that are involved in the provision of a designated service, including any functions carried out by a responsible third party. Coin Harbour does not currently engage any responsible third parties to carry out any functions as outlined in part A of the Program.

12.2 The procedures in Part A apply on and from 6-June-2021.

13. THE AML/CTF COMPLIANCE OFFICER

13.1 Coin Harbour has appointed Peter Cooney as its AML/CTF Compliance Officer.

13.2 Where Peter Cooney is absent the role and responsibilities of the AML/CTF Compliance Officer will be delegated to Director Kent Kingsley.

13.3 Coin Harbour's AML/CTF Compliance Officer is:

(a) the AML/CTF Compliance Officer for the purposes of the AML/CTF Act and Rules; and

(b) appointed by Coin Harbour as its Nominated Contact Officer for the purposes of the AML/CTF Rules.

13.4 The AML/CTF Compliance Officer will at all times:

(a) be part of the management of Coin Harbour;

(b) report directly to the Director of Coin Harbour; and

(c) possess sufficient skills and experience to carry out the role of the AML/CTF Compliance Officer.

13.5 The AML/CTF Compliance Officer is responsible for implementing and over-seeing Coin Harbour's obligations under the AML/CTF Act and Rules in accordance with Coin Harbour's compliance procedures.

13.6 The AML/CTF Compliance Officer is authorised to delegate any of its responsibilities under this Program, the AML/CTF Act or Rules to another Coin Harbour employee, agent or responsible third party provided it is reasonable to do so. The AML/CTF Compliance Officer's responsibilities are to be undertaken in conjunction with an external compliance consultant.

14. EMPLOYEE DUE DILIGENCE PROGRAM

14.1 Coin Harbour does not have any existing employees who are currently in a position to facilitate the commission of a money laundering or terrorism financing offence.

14.2 **New Employees**

(a) The AML/CTF Compliance Officer must be informed of all prospective new employees before they are issued with an employment contract.

(b) For all newly created roles or previously existing roles that are to be filled with a new employee, a risk assessment must be undertaken of that role to determine whether they will be in a position to facilitate the commission of a money laundering or terrorism financing offence.

(c) In respect to all prospective employees who, if employed (to fill a newly created role that is able to facilitate a money laundering or terrorism financing transaction, or a previously-existing role that is now able to facilitate a money laundering or terrorism financing transaction), may be in a position to facilitate the commission of a money laundering or terrorism financing offence in connection with the provision of a designated service, the AML/CTF Compliance Officer will:

(i) collect information about and verify the identity of the employee in accordance with Part B as if they were a new individual customer;

(ii) obtain a copy of the prospective employee's 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, if none, the person's highest educational qualification;

(v) carry out a criminal history check with the Australian Federal Police (**"AFP"**) (subject to 14.2(e) below); and

(vi) carry out a bankruptcy/credit check;

(d) Steps (i), (ii) and (iii) in Section 14.2(c) of this Program will be carried out for all prospective employees regardless of their position at Coin Harbour.

(e) Steps (iv), (v) and (vi) in Section 14.2(c) this Program will be carried out at the discretion of the AML/CTF Compliance Officer having regard to the money laundering or terrorism financing risk associated with the position of the prospective employee.

(f) The procedures in Section 14.1 of this Program will be carried out before an employment offer is made unless the AML/CTF Compliance Officer decides otherwise having regard to the reason(s) why they cannot be completed beforehand and the money laundering or terrorism financing risk associated with the position of the prospective employee.

(g) If a prospective employee fails, without reasonable excuse, to comply with these procedures, then Coin Harbour may decide not to offer that person employment.

(h) Employment contracts issued after 6-June-2021will include a clause stating that employment within Coin Harbour is conditional on passing the checks outlined in this Program.

(i) If an offer of employment has already been made, and the prospective employee does not co-operate with the above procedures or the results of the checks are not satisfactory, then Coin Harbour may withdraw the offer.

14.3 **Existing Employees**

(a) Where it is proposed that an employee will be transferred or promoted to a new role, a risk assessment must be undertaken of that role to determine whether they will be in a position to facilitate the commission of a money laundering or terrorism financing offence.

(b) Where an employee is transferred or promoted to a role that may put them in a position to facilitate the commission of a money laundering or terrorism financing offence in connection with the provision of a designated service, the AML/CTF Compliance Officer will:

(i) obtain an updated copy of the employee's visa where the employee is not an Australian citizen; and

(ii) carry out any other identification, reference, criminal history checks with the AFP or credit checks that are deemed necessary by the AML/CTF Compliance Officer.

(c) Employees who fail to comply with the procedures above will be reported to Coin Harbour's Compliance Officer. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

14.4 Copies of employee checks undertaken in accordance with Sections 14.2 and 14.3 of this Program will be kept in accordance with the Coin Harbour's Document Retention Policy.

14.5 **Managing Non-Compliance**

(a) Coin Harbour will, on an ongoing basis, monitor its employees' compliance with this Program.

(b) The employees' compliance with this Program will be monitored in a number of ways and may include, subject to applicable laws, surveillance of an employee's activities in the workplace.

(c) An employee who fails to comply with this Program will be reported to the AML/CTF Compliance Officer. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

15. RISK AWARENESS TRAINING PROGRAM

15.1 The Risk Awareness Training Program (**"RATP"**) is designed to ensure each employee of Coin Harbour receives appropriate ongoing training on the money laundering and terrorism financing risk that Coin Harbour may face.

15.2 The RATP is designed to enable Coin Harbour's employees to understand:

(a) Coin Harbour'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 money laundering or terrorism financing risk that Coin Harbour might face and the potential consequences of such risk; and

(d) those processes and procedures provided for by this Program which are relevant to the work carried out by the employee.

15.3 Employees receive training as soon as practicable upon receipt of a copy of this Program. This training also includes training in relation to Coin Harbour's Document Retention Policy.

15.4 **Ongoing Compliance Training**

(a) An external compliance consultant provides regular updates on compliance issues, including AML/CTF and AUSTRAC issues.

(b) These updates are made available to all employees of Coin Harbour.

15.5 **Employee AML/CTF Seminars**

(a) The AML/CTF Compliance Officer will organise AML/CTF seminars covering the AML/CTF issues faced by Coin Harbour. In particular, the seminars will cover issues in Section 15.2(c) and 15.2(d) of this Program.

(b) The AML/CTF seminars will be conducted as determined by the AML/CTF Compliance Officer. For new employees and employees on leave, a separate seminar may be conducted within a reasonable time of commencing employment if the AML/CTF Compliance Officer determines it is necessary having regard to the money laundering or terrorism financing risk associated with the position of the existing or prospective employee.

(c) A record will be kept of each employee who attends an AML/CTF seminar in accordance with Coin Harbour's Document Retention Policy.

(d) At the discretion of the AML/CTF Compliance Officer, additional seminars will be conducted to ensure that all employees remain aware of and up-to-date with changes in the AML/CTF legislation and requirements.

(e) Non-attendance at an AML/CTF seminar by an employee, without reasonable excuse, will be reported to the Director and appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Officer.

(f) From time to time some employees, depending on the nature of their role and responsibilities, may be required to undertake additional training as directed by the AML/CTF Compliance Officer.

(g) The AML/CTF Compliance Officer will make available to all employees a current copy of this Program.

15.6 **Document Retention Policy**

(a) The AML/CTF Compliance Officer will require each:

(i) new employee to read a copy of Coin Harbour's Document Retention Policy within a reasonable time of commencing their employment; and

(ii) employee to read a copy of Coin Harbour's Document Retention Policy on a regular basis as determined by the AML/CTF Compliance Officer.

(b) Employees who fail, without reasonable excuse, to read Coin Harbour's Document Retention Policy will be reported to the Director. Appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Officer.

16. OUTSOURCING

16.1 Coin Harbour does not currently outsource any of its AML/CTF obligations.

16.2 The only exception to this is that Coin Harbour subscribes to the KYCAid platform for electronic API access to the Document Verification Service (DVS).

16.3 Where Coin Harbour outsources any of its AML/CTF obligations, it will: / If Coin Harbour outsources any of its AML/CTF obligations in the future, it will:

(a) have an agreement in place with the party to whom the activities are outsourced;

(b) where relevant, require the parties to whom the activities are outsourced to implement the policies and procedures outlined in this AML/CTF Program;

(c) assess the money laundering or terrorism financing risk associated with the outsourcing of the particular activity;

(d) conduct due diligence on the activities outsourced to ensure that outsourcing these activities and services is not increasing the money laundering or terrorism financing risk faced by Coin Harbour;

(e) conduct due diligence on the parties to whom the activities are outsourced to ensure that outsourcing activities to these parties is not increasing the money laundering or terrorism financing risk faced by Coin Harbour;

(f) ensure that all parties to whom the activities and services are outsourced understand:

(i) Coin Harbour'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 money laundering or terrorism financing risk Coin Harbour might face and the potential consequences of such risk; and

(iv) those processes and procedures provided for by this Program that are relevant to the work carried out by the employee.

16.4 Where Coin Harbour outsources its customer identification procedures as described in Part B of this Program to a third party under any circumstances it will:

(a) conduct due diligence on the third party to ensure they hold the appropriate licences and/or registrations with ASIC, AUSTRAC or any other relevant regulator;

(b) have an agreement in place with the third party to whom the activities are outsourced;

(c) ensure the third party has an AML/CTF policy in place which complies with the AML/CTF Rules;

(d) ensure the agreement in place between Coin Harbour and the third party provides Coin Harbour access to the KYC records of its clients;

(e) conduct due diligence on the activities outsourced to ensure that outsourcing these activities and services is not increasing the money laundering or terrorism financing risk faced by Coin Harbour.

16.5 Coin Harbour will assess the ML/TF risk associated with a third party undertaking customer identification procedures on its behalf having regard to the following factors:

(a) the existence and quality of the third party's AML/CTF Program;

(b) the resources of the third party, including the number of staff and access to technological resources;

(c) the outcome of due diligence undertaken in respect of the third party; and

(d) quotes received and references from former and current partners of the third party.

16.6 The following services relating to Coin Harbour's AML/CTF obligations will be outsourced:

(a) Client Identification and Verification (during on boarding) – KYCAid

17. PROVISION OF DESIGNATED SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES

17.1 Coin Harbour does not provide designated services through permanent establishments in foreign countries.

17.2 If at any time Coin Harbour begins to provide designated services at or through permanent establishments in foreign countries, the AML/CTF Compliance Officer will determine which parts of this Program will apply to the permanent establishments and will amend this Program accordingly.

18. RECORD KEEPING OBLIGATIONS RELATING TO CUSTOMER IDENTIFICATION AND THE PROVISION OF DESIGNATED SERVICES

18.1 When a customer identification procedure is required to be undertaken in accordance with Part B of this Program, a record of the following must be made:

(a) the procedures undertaken; and

(b) information obtained in the course of carrying out the procedures.

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

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

(a) to provide the record to an AUSTRAC authorised officer within a reasonable period; and

(b) to demonstrate to the AUSTRAC authorised officer that the reporting entity has complied with the obligations under subsection 112(2) of AML/CTF Act.

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

19. TRANSACTION MONITORING

19.1 Coin Harbour has a transaction risk-based monitoring process to identify suspicious transactions which have no economic or lawful purpose. These include:

(a) complex transactions;

(b) unusual and large transactions;

(c) unusual patterns of transactions;

(d) multiple transactions involving a range of digital currencies; and/or

(e) digital currencies that pose a higher ML/TF risk or provide greater anonymity.

19.2 Coin Harbour's transaction monitoring system consists of three steps:

(a) Monitoring all customer transactions in accordance with Coin Harbour's policies, systems and procedures;

(b) Identify all suspicious transactions; and

(c) Take the appropriate actions, including but not limited to:

(i) develop customer profiles and identify irregular and unusual patterns of transactions;

(ii) identify rapid exchange of currencies;

(iii) identify rapid movement of funds; and

(iv) identify interactions with known mixers, the use of high-risk counterparties and transactions that use the dark net.

19.3 All Coin Harbour employees receive training to be vigilant in monitoring suspicious matters. Under Section 15 of this Program, employees receive appropriate ongoing training on the money laundering or terrorism financing risk that Coin Harbour may face.

19.4 The following table provides a summary of the reporting obligations of Coin Harbour and the systems and controls in place to ensure compliance.

Coin Harbour's Reporting Obligations					
Compliance Obligations	**Reference**	**Requirements to maintain Compliance**	**Compliance Action**	**Responsible Officer**	**Frequency**
AML/CTF Compliance Reports	AML/CTF Part 3, Division 5	Submit compliance report to AUSTRAC	Ensure that AML/CTF Compliance reports are completed in line with AUSTRAC regulations and are submitted accordingly.	AML/CTF Compliance Officer	Annually
Changes to Coin Harbour's AUSTRAC enrolment and/or registration	AML/CTF Part 3A	Notify AUSTRAC of change in enrolment and/or registration details	Ensure that changes to Coin Harbour's enrolment and/or registration details are reported to AUSTRAC within fourteen (14) days.	AML/CTF Compliance Officer	As required
Suspicious Matter Reporting	AML/CTF Part 3, Division 2 and 6	Implement and monitor SMR procedures	Ensure all SMRs are reported to AUSTRAC within the appropriate time frame. An SMR must be submitted within three (3) business days of forming the suspicion. If the suspicion relates to the financing of terrorism, the SMR must be submitted within twenty-four (24) hours of forming the suspicion	AML/CTF Compliance Officer	As required
Threshold Transaction Reporting	AML/CTF Part 3, Division 3 and 6	Implement and monitor TTR procedures	Ensure all TTRs are reported to AUSTRAC within ten (10) business days of the threshold transaction taking place.	AML/CTF Compliance Officer	As required

19.5 Coin Harbour has implemented the following systems and controls to ensure compliance with the reporting obligations in section 19.4:

(a) Coin Harbour's Director maintains overall responsibility for all reporting obligations and the AML/CTF Compliance Officer is responsible for completing and lodging the reports within the required timeframes;

(b) **AML/CTF Compliance Reports:** Coin Harbour maintains a compliance calendar which includes a number of key dates to ensure the reporting obligations are lodged within the required timeframes;

(c) **Changes to Coin Harbour's AUSTRAC enrolment or registration details:** the Director is responsible for notifying the AML/CTF Compliance Officer of any changes to Coin Harbour's enrolment or registration details and the AML/CTF Compliance Officer must ensure AUSTRAC is notified within fourteen (14) days. The AML/CTF Compliance Officer conducts monthly reviews of Coin Harbour's enrolment and registration details;

(d) **Suspicious Matter Reports:** Coin Harbour undertakes transaction monitoring as described in section 27 of this Program. Where the AML/CTF Compliance Officer identifies a transaction which is suspicious, they will report the matter to AUSTRAC in accordance with section 20.

(e) **Threshold Transaction Reports:** Coin Harbour undertakes transaction monitoring as described in section 27 of this Program. Where the AML/CTF Compliance Officer identifies a threshold transaction, they will report the matter to AUSTRAC in accordance with section 21.

20. SUSPICIOUS MATTER REPORTING

20.1 If an employee or representative of Coin Harbour suspects that:

(a) an existing, new or potential customer, or the agent of an existing, new or potential customer, is not who they claim to be; or

(b) information about the provision (or prospective provision) of a service to a customer may be:

(i) relevant to the investigation or prosecution of a person for:

(A) an offence against a law of the Commonwealth, a State or Territory;

(B) an evasion, or an attempted evasion, of a taxation law (as defined in the *Taxation Administration Act* 1953 (Cth)) or a law of a State or Territory that deals with taxation; or

(C) a money laundering or terrorism financing offence;

(ii) of assistance in the enforcement of laws relating to proceeds of crime; or

(iii) the provision of a service to a customer may be preparatory to the commission of a money laundering or terrorism financing offence,

the employee who forms the suspicion must **immediately** notify the AML/CTF Compliance Officer of their suspicion.

20.2 Upon receiving a notification from an employee or representative under Section 20.1 of this Program, the AML/CTF Compliance Officer must assess the information which led the employee to form a suspicion and determine whether a Suspicious Matter Report should be lodged.

20.3 If the AML/CTF Compliance Officer determines that a Suspicious Matter Report must be lodged in relation to a customer, Coin Harbour will:

(a) apply the enhanced customer due diligence program outlined in this Program; and

(b) report the suspicion to AUSTRAC's CEO by submitting a Suspicious Matter Report via Coin Harbour's AUSTRAC Online Account:

(i) within twenty-four (24) hours after the time when the AML/CTF Compliance Officer forms the relevant suspicion, if the matter relates to terrorism financing; or

(ii) in all other cases, within three (3) business days after the time when the AML/CTF Compliance Officer forms the relevant suspicion.[1]

20.4 Upon receiving a notification under Section 20.1(a) of this Program relating to the identity of the customer, the AML/CTF Compliance Officer must, within fourteen (14) days, do one (1) of the following for the purpose of enabling Coin Harbour to be reasonably satisfied that the customer is the person that he or she claims to be:

(a) collect additional Know Your Customer (**"KYC"**) Information in respect of the customer;

(b) re-verify, from a reliable and independent source, any KYC Information that has been obtained in respect of the customer; or

(c) verify, from a reliable and independent source, any previously unverified KYC Information that has been obtained in respect of the customer.[2]

20.5 If:

(a) after collecting additional KYC Information from a customer in accordance with Section 20.4 of this Program, the AML/CTF Compliance Officer is still not satisfied that the customer is who they claim to be; or

(b) the AML/CTF Compliance Officer is unable to collect any additional information from the customer,

then the AML/CTF Compliance Officer must make a Suspicious Matter Report to AUSTRAC.

[1] Section 42(3)(a) of the AML/CTF Act

[2] Section 35 of the AML/CTF Act; Rules Part 6.2.

20.6 If the AML/CTF Compliance Officer makes a Suspicious Matter Report to AUSTRAC in relation to a customer, the AML/CTF Compliance Officer must also consult with AUSTRAC and other relevant enforcement agencies to determine how best to deal with the customer.

20.7 Reporting suspicious matters is subject to 'tipping off' provisions. It is an offence under section 123 of the AML/CTF Act for a reporting entity, or an employee of a reporting entity, to let the person about whom you formed the suspicion, another person, or organisation:

(a) know that an SMR has been reported to AUSTRAC;

(b) know that a reportable suspicion has been formed regarding a particular matter;

(c) infer that a suspicion has been made; and

(d) know that information and/or documentation has been supplied to AUSTRAC.

20.8 Under no circumstances should the employee or representative discuss the matter with any person other than their immediate supervisor, unless authorised by the AML/CTF Compliance Officer. This is described as the offence of 'tipping off' and is prohibited under the AML/CTF Act.

20.9 Under section 123 of the AML/CTF Act, if:

(a) a suspicious matter reporting obligation arises or has arisen for Coin Harbour in relation to a person; and

(b) Coin Harbour has communicated the information to the AUSTRAC CEO under their suspicious matter reporting obligations;

Coin Harbour must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC that the information has been communicated to the AUSTRAC CEO.

20.10 Coin Harbour must continue to transact with the customer on the usual basis until further advised by AUSTRAC and other relevant enforcement agencies.

20.11 A report to AUSTRAC's CEO of any of the matters set out at Section 20.1 of this Program must be in the approved form and sent in accordance with the requirements of Section 41 of the AML/CTF Act and Chapter 18 of the AML/CTF Rules.

20.12 A representative of Coin Harbour must not disclose to someone other than AUSTRAC's CEO or an AUSTRAC staff member:

(a) that Coin Harbour has reported, or is required to report, information to AUSTRAC's CEO under section 41 of the AML/CTF Act;

(b) that Coin Harbour has formed a suspicion, under section 41 of the AML/CTF Act, about a transaction or matter;

(c) any other information from which the person to whom the information is disclosed could reasonably be expected to infer that information has been communicated to AUSTRAC's CEO under section 41 of the AML/CTF Act or the suspicion has been formed; or

(d) that information or documentation has been given or produced under section 49 of the AML/CTF Act.

20.13 If the AML/CTF Compliance Officer, on behalf of Coin Harbour, forms a reasonable suspicion relating to one of the matters set out in Section 20.1 of this Program in respect of an existing customer (that is, a person who was a customer of Coin Harbour as at 12 December 2007), the AML/CTF Compliance Officer must, within fourteen (14) days commencing after the day on which the AML/CTF Compliance Officer formed the suspicion, carry out the applicable customer identification procedures in Part B of this Program unless the AML/CTF Compliance Officer determines that Coin Harbour has previously carried out or been deemed to have carried out that procedure or a comparable procedure.

20.14 The AML/CTF Compliance Officer must examine the background, purpose and circumstances of suspicious matters that they have detected and reported and determine whether any changes should be made to this Program. This should occur periodically (at least annually) and whenever a particularly unusual suspicious matter is identified.

21. THRESHOLD TRANSACTION REPORTS ("TTR")

21.1 In this Section:

(a) 'Physical currency' is the coin or printed money of Australia or another country which is designated as legal tender; and

(b) 'Digital currency' means:

(i) a digital representation of value that:

(A) functions as a medium of exchange, a store of economic value, or a unit of account; and

(B) is not issued by or under the authority of a government body; and

(C) 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

(D) is generally available to members of the public without any restriction on its use as consideration; or

(ii) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;

but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of the AML/CTF Act.

(c) 'Digital currency wallet' means any service that allows a person to send, request, receive, or store digital currency; and

(d) 'Unique device identifiers' includes Media Access Control (MAC) addresses, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) numbers, and secure element ID (SEID) numbers.

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

21.3 All employees of Coin Harbour must notify the Compliance Officer of any transactions relating to 'physical currency' or 'digital currency' with a value of AUD10,000 or more (or the foreign currency equivalent) immediately.

21.4 When the AML/CTF Compliance Officer receives a notification from an employee of Coin Harbour regarding a threshold transaction, the AML/CTF Compliance Officer will submit a TTR to the AUSTRAC CEO within ten (10) business days of the threshold transaction taking place.

21.5 A report to AUSTRAC in relation to the TTR must be in the approved form and sent in accordance with the requirements of the AML/CTF Rules. These include:

(a) The date of the threshold transaction;

(b) A description of the designated service provided or commenced to be provided by the Reporting Entity to the customer which involves the threshold transaction;

(c) The total of the funds provided to or received from the customer.

(d) Details of the threshold transaction, including whether it involved physical currency or digital currency.

21.6 If the customer of the designated service is an individual, the details required in the TTR include:

(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 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;

(i) if the person conducting the threshold transaction is not the customer, the details for the person specified in part 21.6(a) and if applicable, part 21.6(b) and 21.6(c).

21.7 If the customer conducting the transaction is a business, the details required in the TTR include:

(a) The name of the customer and any business name(s) under which the customer operates;

(b) A description of the legal form of the customer and any business structure it is a part of, if known;

(c) The full address of the customer's principle place of business;

(d) The postal address of the customer if different from the full address;

(e) The ACN, ARBN and/or ABN of the customer, if known;

(f) The customer's telephone number, if known;

(g) The details of the person conducting the threshold transaction.

21.8 Where the threshold transaction involves physical currency, all of the following details as applicable to the threshold transaction are also required to be provided in the TTR:

(a) the total amount in Australian dollars;

(b) if the amount involves foreign currency, a description and amount of the currency;

(c) the name(s) of the recipient(s);

(d) the full address(es) of the recipient(s) (not being a post box address), if known;

(e) the date(s) of birth of the recipient(s), if known;

(f) a description of the purpose of the transfer(s);

(g) if the purpose of the transfer(s) is to:

(i) enable a cheque to be provided to the customer using all or part of the physical currency transferred by the customer; or

(ii) enable the customer to receive physical currency in exchange for all or part of a cheque produced by the customer to the reporting entity;

the following details:

(iii) the name of the drawer;

(iv) the name of the drawee; and

(v) the amount of the cheque;

21.9 Where the threshold transaction involves digital currency, all of the following details as applicable to the threshold transaction are also required to be provided in the TTR:

(a) the denomination or code of the digital currency and the number of digital currency units;

(b) the value of the digital currency involved in the transaction, expressed in Australian dollars, if known;

(c) a description of the digital currency including details of the backing asset or thing, if known;

(d) the name(s) of the recipient(s);

(e) the full address(es) of the recipient(s) (not being a post box address), if known;

(f) the date(s) of birth of the recipient(s), if known;

(g) a description of the purpose of the transfer(s);

(h) if the purpose of the transfer(s) is to:

(i) enable a cheque to be provided to the customer using all or part of the digital currency transferred by the customer; or

(ii) enable the customer to receive digital currency in exchange for all or part of a cheque produced by the customer to the reporting entity;

(iii) the following details:

(iv) the name of the drawer;

(v) the name of the drawee; and

(vi) the amount of the cheque;

(i) the Internet Protocol (IP) address information of the customer and the recipient(s), if known;

(j) the email address of the customer and the recipient(s), if known;

(k) the mobile phone number of the customer and the recipient(s), if known;

(l) the social media identifiers of the customer and the recipient(s), if known;

(m) the unique identifiers relating to the digital currency wallet(s) of the customer and the recipient(s), if known; and

(n) the unique device identifiers of the customer and the recipient(s), if known.

22. AML/CTF COMPLIANCE REPORTS

22.1 Coin Harbour is required to submit an AML/CTF Compliance Report to AUSTRAC by the specified due date. AUSTRAC will inform Coin Harbour of the AML/CTF Compliance report due date.

22.2 An AML/CTF Compliance Report outlines the appropriateness of Coin Harbour's AML/CTF risk assessment and the effectiveness of Coin Harbour's AML/CTF program.

23. CHANGES TO COIN HARBOUR'S AUSTRAC ENROLMENT/REGISTRATION DETAILS

23.1 Part 8.9.1 of the AML/CTF Rules outlines the requirements of Coin Harbour to report to AUSTRAC any material changes in circumstances and other specified circumstances under section 75M of the AML/CTF Act; and

23.2 Chapter 60 of the AML/CTF Rules outlines the changes in registration details Coin Harbour must report to AUSTRAC. These include:

(a) changes to Coin Harbour's registration details;

(b) changes in the number of key personnel at Coin Harbour and a declaration that a police and bankruptcy checks have been obtained;

(c) whether any key personnel of Coin Harbour have been criminally charged;

(d) whether Coin Harbour is the subject of a civil penalty issued under the AML/CTF Act; and

(e) whether Coin Harbour is the subject of civil or criminal proceedings or enforcement action.

23.3 Coin Harbour as a Digital Currency Exchange Provider is required to notify AUSTRAC of a change in Coin Harbour's circumstances within fourteen (14) days of the change in detail.

23.4 Changes to Coin Harbour's AUSTRAC details should be completed electronically through Coin Harbour's AUSTRAC Online account.

23.5 Chapter 64 of the AML/CTF Rules outlines the changes in enrolment details Coin Harbour must report to AUSTRAC changes in the enrolment details set out in Part A of the Schedule of Chapter 63 of the Rules.

23.6 Notification of a change of Coin Harbour's enrolment details may be made by an agent of Coin Harbour where:

(a) there is a current written agreement in place between the agent of Coin Harbour and Coin Harbour, or Coin Harbour has provided to the agent of Coin Harbour a written authority;

(b) that agreement or written authority authorises the agent to notify, on behalf of Coin Harbour, a change in the enrolment details of Coin Harbour on the Reporting Entities Roll; and

(c) the notification of a change in Coin Harbour's enrolment details includes a declaration by the agent that the information is true, accurate and complete.

24. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

24.1 Where Coin Harbour has provided or is providing a designated service to a customer and the AML/CTF Compliance Officer believes, on reasonable grounds, that a customer has information that may assist Coin Harbour in the identification, management and mitigation of money laundering or terrorism financing risk, the AML/CTF Compliance Officer may request the customer to provide Coin Harbour with any such information. The request must be provided in writing and notify the customer that if the request is not complied with, then Coin Harbour may do any or all of the following until the information, covered by the request, is provided:

(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 to the customer.

24.2 If the customer does not comply with the request within a reasonable time then the AML/CTF Compliance Officer may determine that, until the information covered by the request is provided, Coin Harbour will:

(a) refuse to continue to provide the designated service;

(b) refuse to commence to provide the designated service; or

(c) restrict or limit the provision of the designated service to the customer.

24.3 In these circumstances, the AML/CTF Compliance Officer will determine whether the matter should be reported to AUSTRAC as a suspicious matter (refer to Section 20 of this Program).

25. ONGOING CUSTOMER DUE DILIGENCE – OVERVIEW

25.1 Coin Harbour will monitor its customers with a view to identifying, mitigating and managing the risk that the provision of a designated service at or through a permanent establishment in Australia may involve or facilitate money laundering or terrorism financing.

25.2 Coin Harbour has identified the following customer types that it will provide services to when determining its AML/CTF Risk

(a) Individuals;

(b) Companies;

(c) Trusts;

25.3 Coin Harbour has identified the following customer types that it does not currently provide services to but may provide services to in the future:

(a) Individuals;

(b) Companies;

(c) Trusts;

(d) Trustees and beneficiaries;

(e) Partnerships;

(f) Associations;

(g) Registered cooperatives;

(h) Government bodies; and

(i) Agents.

25.4 Coin Harbour will monitor its customers by implementing systems to:

(a) collect further KYC Information for ongoing customer due diligence processes;

(b) update and verify KYC Information for ongoing customer due diligence purposes;

(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.

25.5 As part of implementing systems for ongoing customer due diligence purposes, Coin Harbour will group its customers according to their level of risk assessed as part of the risk assessment procedures outlined in this Program. The risk grouping will determine:

(a) what further KYC Information needs to be collected for ongoing customer due diligence purposes in respect of a particular customer;

(b) what level of transaction monitoring needs to be conducted in relation to a customer; and

(c) whether the enhanced customer due diligence program needs to be applied.

26. ADDITIONAL KYC INFORMATION

26.1 In undertaking the risk assessment for new activities and technologies referred to in Section 11 of this Program, the AML/CTF Compliance Officer will determine whether any additional KYC Information or Beneficial Owner information should be collected from relevant customers either before any designated services are provided to the customer or during the course of Coin Harbour's relationship with the customer. These requirements will be incorporated into the relevant customer procedures.

26.2 Based on the assessed level of the money laundering and terrorism financing risk involved in the provision of designated services provided by Coin Harbour on the date that this Section of this Program was adopted, Coin Harbour has determined that no additional KYC Information needs to be collected in relation to low risk customers. The AML/CTF Compliance Officer will determine what additional KYC Information or Beneficial Owner information will be collected, in respect of medium and high risk customers, prior to the provision of any designated service to assist Coin Harbour to undertake ongoing customer due diligence.

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

26.4 In respect of an existing customer, Coin Harbour will update and re-verify KYC Information by requesting additional KYC Information where the AML/CTF Compliance Officer considers the KYC Information is no longer up-to-date, incomplete or unreliable. Coin Harbour will also request additional KYC information where the scope of the services provided to an existing customer changes.

26.5 Coin Harbour will update and re-verify KYC Information in respect of a customer where:

(a) the AML/CTF Compliance Officer considers that KYC Information held in respect of a customer or Beneficial Owner is likely to be incomplete or unreliable;

(b) a representative of Coin Harbour becomes aware that KYC Information held in respect of a customer or Beneficial Owner has or is likely to have changed;

(c) the customer engages in a significant transaction or series of transactions with one or more reporting entities, 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

(d) a significant change occurs in the way the customer conducts transactions, where a significant change occurs if the number of transactions carried out by a customer increases by 100% within a five (5) calendar day period.

26.6 Where one of the above circumstances arises in respect of a customer and the applicable customer identification procedure has not previously been carried out in respect of a customer (i.e. the customer is a pre-commencement customer), Coin Harbour will carry out the applicable customer identification procedure in accordance with Part B of this Program and collect the relevant additional KYC Information.

26.7 Where a change in customer information relates to in the case of:

(a) individual customers, the customer's:

(i) name; or

(ii) residential address;

(b) a company:

(i) the company's name; or

(ii) the company's registration number;

(c) a trust:

(i) the trustee; or

(ii) the name of the trust; and

(d) in the case of a partnership, the identity of a partner.

26.8 Coin Harbour will seek to verify the updated KYC Information using reliable and independent documentation in accordance with Section 62 of this Program.

27. TRANSACTION MONITORING PROGRAM

27.1 This Section describes the transaction monitoring program adopted by Coin Harbour which includes risk-based systems and controls to monitor the transactions of customers, for the purpose of identifying any transaction that appears to be suspicious under section 41 of the AML/CTF Act (refer to Section 20 of this Program).

27.2 The Director has overall responsibility and oversight of Coin Harbour's transaction monitoring program. Coin Harbour conducts transaction monitoring on a daily basis.

27.3 The AML/CTF Compliance Officer must identify money laundering and terrorism financing risk factors relevant to customers of particular services and products provided by Coin Harbour, which may involve the provision of a designated service and to representatives of such customers. Such risk factors include the:

(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 the lists maintained by the

Department of Foreign Affairs and Trade under the Charter of United Nations (Terrorism and Dealings with Assets) Regulations 2002 (Cth); or

(d) transaction involves a customer or third party who is a PEP (refer to Section 68 of this Program).

27.4 In addition to the Risk Awareness Training referred to in Section 15 of this Program, the AML/CTF Compliance Officer will ensure that all employees of Coin Harbour, who have direct contact with customers or their representatives, receive regular training in the identification of relevant money laundering or terrorism financing risk factors.

27.5 An employee of Coin Harbour must immediately inform the AML/CTF Compliance Officer when any money laundering or terrorism financing risk factor(s) are identified in relation to a customer or a customer's representative.

27.6 The AML/CTF Compliance Officer will then liaise with Coin Harbour's Director in relation to any further action by Coin Harbour including, but not limited to the items actions listed in 27.8.

27.7 Where an employee of Coin Harbour identifies a customer or third party of a kind specified in Section 27.3(c) or 27.3(d) of this Program, the AML/CTF Compliance Officer will take such appropriate action as is necessary, including seeking further information from the customer or their representative or from another source, to determine, with a reasonable degree of certainty, whether the customer or third party is that person.

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

(a) a customer should be placed in a higher risk grouping, Coin Harbour will collect additional KYC Information if required as referred to in Section 26 of this Program;

(b) KYC Information needs to be updated or verified in respect of a customer, Coin Harbour will update or verify the required information in accordance with Section 26 of this Program;

(c) a customer is a high risk customer, Coin Harbour will apply the enhanced customer due diligence program in accordance with Section 28 of this Program; or

(d) a suspicious matter report needs to be lodged in respect of a customer, Coin Harbour will follow the procedure outlined in Section 20 of this Program.

27.9 The AML/CTF Compliance Officer, in consultation with the Director, must regularly assess Coin Harbour's transaction monitoring program and should take steps to have this Program modified appropriately:

(a) where there has been a significant change in the money laundering or terrorism financing risk relating to designated services provided by Coin Harbour;

(b) prior to Coin Harbour introducing a new designated service to the market;

(c) prior to Coin Harbour adopting a new method of delivering a designated service;

(d) prior to Coin Harbour adopting a new technology or developing technology used for the provision of an existing or new designated service; and

(e) where the AML/CTF Compliance Officer identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of Coin Harbour's customers.

28. ENHANCED CUSTOMER DUE DILIGENCE PROGRAM

28.1 Where the AML/CTF Compliance Officer determines that:

(a) the money laundering or terrorism financing risk associated with a particular designated service, customer, delivery method or jurisdiction is high, including but not limited to when the customer:

(i) is engaged in business which involves a significant number of cash transactions or amounts of cash;

(ii) uses a complex business ownership structure for no apparent commercial or other legitimate reason, especially if the Beneficial Owners of the legal entity cannot be determined;

(iii) is based in, or conducts business through or in, a high-risk jurisdiction;

(iv) cannot provide information to verify the source of funds;

(v) requests an undue level of secrecy in relation to a designated service;

(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 20 of this Program);

(d) Coin Harbour 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.

28.2 Where one or more of the circumstances in Section 28.1 arises the AML/CTF Compliance Officer will arrange for one or more of the following due diligence procedures to occur:

(a) seek further information from the customer or from third party sources in order to:

(i) clarify or update the customer's KYC Information or Beneficial Owner information already collected from the customer, in accordance with Section 26 of this Program;

(ii) obtain any further KYC Information or Beneficial Owner information in accordance with Section 26 of this Program, including where appropriate, 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 Coin Harbour.

(b) conduct more detailed analysis in respect of the customer's KYC Information and Beneficial Owner information taking reasonable measures to identify:

(i) the source of the customer's and each Beneficial Owner's wealth; and

(ii) the source of the customer's and each Beneficial Owner's funds;

(c) verify or re-verify KYC Information or Beneficial Owner information in accordance with the customer identification program outlined in Part B of this Program;

(d) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future, including but not limited to:

(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 in accordance with section 41 of the AML/CTF Act (refer to Section 20 of this Program);

(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 to the customer; and

(g) consider whether a transaction or particular transactions should be processed.

29. REVIEW OF COIN HARBOUR'S AML/CTF PROGRAM

29.1 The AML/CTF Compliance Officer must regularly assess Coin Harbour's money laundering or terrorism financing risk and should take steps to have this Program modified appropriately:

(a) where the AML/CTF Compliance Officer identifies that there has been a significant change in the money laundering or terrorism financing risk relating to designated services provided by Coin Harbour;

(b) prior to Coin Harbour introducing a new designated service to the market;

(c) prior to Coin Harbour adopting a new method of delivering a designated service;

(d) prior to Coin Harbour adopting a new technology or developing technology used for the provision of an existing or new designated service; and

(e) where the AML/CTF Compliance Officer identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of Coin Harbour's customers.

29.2 Due to the small number of staff members at Coin Harbour, internal reviews will not be carried out internally unless the AML/CTF Compliance Officer considers it necessary or subject to Section 29.2 of this Program. Internal reviews may be carried out where required by an independent internal party.

29.3 An independent review of Coin Harbour's AML/CTF Program must take place on an annual basis by either an internal or external party.

29.4 Coin Harbour must ensure that the independent party conducting the review is independent and:

(a) has not been involved in undertaking any of the functions or measures required to be carried out under this Program;

(b) has not been involved in the design, development, implementation, maintenance or management of this Program;

(c) has not been involved in the development of Coin Harbour's risk assessment or related internal controls;

(d) has access to the employees of Coin Harbour and is able to make enquiries of any employee; and

(e) has access to the records, personnel and property of Coin Harbour within the context of Coin Harbour's obligations under the Privacy Act 1988; and

(f) be impartial and objective in performing their duties and should not be inappropriately influenced by management of Coin Harbour; and

(g) be appropriately qualified to conduct the review.

29.5 The AML/CTF Compliance Officer will report the results of the independent review to the Board of Directors of Coin Harbour.

29.6 The independent party, in the course of carrying out the independent review, will:

(a) assess the effectiveness of Part A of this Program having regard to the money laundering or terrorism financing risk of Coin Harbour;

(b) assess whether Part A of this Program complies with the AML/CTF Rules;

(c) assess whether Part A of this Program has been effectively implemented; and

(d) assess whether Coin Harbour has complied with Part A of this Program.

29.7 The independent party, in the course of carrying out the independent review, may also:

(a) assess the risk management resources available to Coin Harbour including, but not limited to:

(i) funding; and

(ii) staff allocation;

(b) identify any future needs relevant to the nature, size and complexity of Coin Harbour; and

(c) assess the ongoing risk management procedures and controls in order to identify any failures.

29.8 When assessing ongoing risk management procedures and controls in order to identify any failures, the independent party conducting the review may have regard to:

(a) any market information relevant to the global AML/CTF environment which may have an impact on the money laundering or terrorism financing risk faced by Coin Harbour;

(b) failure to include all mandatory legislative components in Coin Harbour's AML/CTF Program;

(c) failure to gain approval from Coin Harbour's Director of this Program;

(d) insufficient or inappropriate employee due diligence;

(e) frequency and level of risk awareness training not aligned with potential exposure to AML/CTF risk(s);

(f) changes in business functions which are not reflected in this Program (for example, the introduction of a new product or distribution channel);

(g) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);

(h) failure to undertake an independent review (at an appropriate level and frequency) of the content and application of this Program;

(i) legislation incorrectly interpreted and applied in relation to a customer identification procedure;

(j) customer identification and monitoring systems, policies and procedures that fail to:

(i) prompt, if appropriate, for further identification and/or verification to be carried out when the AML/CTF risk posed by a customer increases;

(ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;

(iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;

(iv) take appropriate action where the identification document provided is neither an original nor a certified copy;

(v) recognise foreign identification issued by a high-risk jurisdiction;

(vi) record details of identification documents, for example, the date of issue;

(vii) consult appropriate resources in order to identify high-risk customers;

(viii) identify when an expired or old identification document (for example, a driver's licence) has been used;

(ix) collect any other name(s) by which the customer is known;

(x) be subject to regular review;

(k) lack of access to information sources to assist in identifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers;

(l) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

(i) customer identification policies, procedures and systems; and

(ii) identifying potential AML/CTF risks;

(m) assess the acceptance of documentation that may not be readily verifiable.

29.9 If the independent party determines it is appropriate, the review may also:

(a) assess whether the risk-based procedures and processes adopted in this Program have changed such that alterations need to be made to this Program;

(b) assess whether Part B of this Program is sufficient to cover the money laundering or terrorism financing risks posed by existing and potential customers of Coin Harbour; and

(c) assess whether any additional changes need to be made to this Program as a result of changes to AML/CTF regulations and legislation and the AML/CTF environment generally.

30. AUSTRAC FEEDBACK

30.1 Where AUSTRAC provides Coin Harbour with feedback regarding performance on the management of money laundering or terrorism financing risk, the AML/CTF Compliance Officer will assess AUSTRAC's feedback to determine if any changes to this Program are required and implement any such changes as soon as reasonably practicable, subject to complying with the procedures in Section 31 of this Program.

30.2 The AML/CTF Compliance Officer will report to the Director of Coin Harbour in relation to any AUSTRAC feedback received and the implementation of any changes required to this Program.

31. OVERSIGHT BY THE BOARD OF DIRECTORS / UPDATING THE PROGRAM

31.1 This Program is approved by the Director of Coin Harbour whilst the Board of Directors is informed of any changes made to this Program.

31.2 The AML/CTF Compliance Officer will report to the Director of Coin Harbour on a regular basis in relation to:

(a) significant changes to the money laundering or terrorism financing risks affecting Coin Harbour’s Reporting Entities;

(b) compliance with this Program, the AML/CTF Act and Rules by Coin Harbour;

(c) the results of and any report produced for any internal or external review of this Program;

(d) any AUSTRAC feedback; and

(e) changes to relevant legislation.

31.3 The AML/CTF Compliance Officer will propose amendments to this Program when required by the Program, AML/CT Act or Rules or as a result of any of the matters in Section 31.2 of this Program. Subject to Section 31.4 of this Program, such amendments should be considered and approved by the Director of Coin Harbour before they become effective.

31.4 The AML/CTF Compliance Officer can implement a change to this Program immediately if the AML/CTF Compliance Officer believes a change needs to be made before the Director's approval can occur. In these circumstances, the AML/CTF Compliance Officer should seek the Director's approval, of a change, as soon as reasonably practical after it is made.

PART B – CUSTOMER IDENTIFICATION

32. INTRODUCTION

32.1 **Part B** of this Program sets out the customer identification procedures for Coin Harbour's customers.

32.2 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 in relation to a customer, having regard to the money laundering or terrorism financing risk relevant to the provision of Coin Harbour's designated services.

32.3 Coin Harbour will consider the following factors when identifying its exposure to money laundering or terrorism financing and developing its customer identification procedures:

(a) its customer types; including:

(i) Beneficial Owners of customers; and

(ii) any politically exposed persons;

(b) Coin Harbour's customers' sources of funds and wealth;

(c) the nature and purpose of the business relationship with its customers, including, as appropriate, the collection of information relevant to that consideration;

(d) the control structure of its non-individual customers;

(e) the types of designated services it provides;

(f) the methods by which it delivers designated services; and

(g) the foreign jurisdiction with which it deals.

33. APPLICATION OF PART B

33.1 Part B of this Program applies to Coin Harbour, including any functions carried out by a responsible third party. Coin Harbour does not currently engage responsible third parties to carry out any functions under Part B of this Program.

34. KYC – CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES

34.1 The customer identification and verification procedures must be carried out by Coin Harbour or a responsible third party:

(a) prior to commencing to provide a designated service to a customer (other than an existing customer), unless Coin Harbour has already carried out the applicable customer identification procedure in respect of the customer; and

(b) when Coin Harbour's employee is responsible for the customer (or another Coin Harbour employee on their behalf), unless the AML/CTF Compliance Officer authorises that these procedures can be conducted by an external party.

34.2 The same KYC procedures will be applied across all Coin Harbour customers in order to ensure that additional procedures do not need to be carried out where a customer uses more than one of Coin Harbour's designated service.

35. KNOW YOUR CUSTOMER – CONSIDERATIONS

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

35.2 In re-assessing the AML/CTF Customer Type Risk for Coin Harbour, it may consider, where appropriate and among other factors, whether:

(a) the customer is unwilling to produce evidence of identification or produces unsatisfactory evidence of identification;

(b) the customer wishes to deal only in large amounts of cash and not in traceable bank transfers;

(c) the customer conducts digital currency exchange transactions very frequently;

(d) there is a high frequency or unusual movement of digital currencies without reasonable explanation;

(e) the amount that the customer exchanges to /from fiat currency is unusually large;

(f) the customer is suspected of presenting false identifications and verification information;

(g) there are any doubts as to whether a customer is acting on their own behalf or whether it appears the customer is fronting on behalf of another person and the 'other' person cannot be identified;

(h) the customer is suspected of undertaking gambling activity using an illegal offshore wagering site;

(i) the customer is suspected of being the perpetrator or is the victim or 'ransomware';

(j) the customer is undertaking transactions involving the 'darknet';

(k) the customer is willing to pay very high charges to complete a transaction;

(l) the customer's normal transaction behaviour changes and they are unwilling to explain the reason for this or the source of the increased funds;

(m) the customer is involved in a complex business ownership structure with no legitimate commercial rationale;

(n) the non-individual customer (for example, a trust, company or partnership) has a complex business structure with little commercial justification, which obscures the identity of the ultimate beneficiaries of the customer;

(o) the customer is in a position which may expose Coin Harbour to the possibility of corruption;

(p) the customer is based in, or conducting business through or in, a high-risk jurisdiction;

(q) the customer is engaged in business which involves significant amounts of cash;

(r) there is no clear commercial rationale for the customer seeking a designated service;

(s) the customer is a PEP;

(t) an undue level of secrecy is requested regarding a designated service;

(u) the situation of the origin of the customer's wealth raises suspicion;

(v) the source of funds is difficult to verify;

(w) the Beneficial Owners of a non-individual customer are difficult to identify and/or verify;

(x) the Beneficial Owners of the non-individual customer are a resident in a high-risk jurisdiction;

(y) there is a one-off transaction in comparison with an ongoing business relationship or series of transactions;

(z) a designated service can be used for money laundering or terrorism financing (and the extent to which it can be used);

(aa) the customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer);

(bb) the customer when migrating from one designated service to another carries a different type and level of AML/CTF risk;

(cc) the customer has income which is not employment-based or from a regular known source;

(dd) the customer is new, rather than having a long-term and active business relationship with Coin Harbour;

(ee) the customer's business is registered in a foreign jurisdiction with no local operations or domicile;

(ff) the customer's business is an unregistered charity, foundation or cultural association;

(gg) the customer is represented by another person, such as under a power of attorney.

36. INDIVIDUALS: CUSTOMER IDENTIFICATION PROCEDURES

36.1 Where a new customer is an individual (other than an individual who notifies Coin Harbour that he or she is a customer in his or her capacity as a sole trader), Coin Harbour:

(a) must collect, at a minimum, the customer's:

(i) full name;

(ii) date of birth; and

(iii) residential address; and

(b) categorises the customer as one of the following:

(i) Individual customer;

(ii) Customers with joint account between husband and wife with a same address;

(iii) Customers with joint account with different surnames but with a same address; or

(iv) Customers with joint account with different addresses.

36.2 Where a new customer notifies Coin Harbour that he or she is a customer in his or her capacity as a sole trader, Coin Harbour must collect, at a minimum, the:

(a) customer's full name;

(b) customer's date of birth;

(c) full business name (if any) under which the customer carries on his or her business;

(d) full address of the customer's principal place of business (if any) or the customer's residential address; and

(e) ABN issued to the customer.

36.3 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular individual is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour's employee to be responsible for the customer. One or more of the following pieces of information will be collected:

(a) any alias names used by the customer;

(b) the customer's occupation or business activities;

(c) the source of the customer's funds including the origin of funds;

(d) income and assets of the customer;

(e) the nature and level of the customer's intended transaction behaviour;

(f) the beneficial ownership of the funds used by the customer/the customer's account with Coin Harbour; and

(g) details of the customer's employment (e.g. name of employer, length of employment, type of institution).

36.4 The information collection requirements in this Section are not intended to conflict with any other obligation Coin Harbour has under other legislation including the *Privacy Act* 1988*.* Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

37. INDIVIDUALS: VERIFICATION – PRINCIPLES

37.1 At a minimum, the following KYC Information about a customer in Section 36, of this Program, must be verified:

(a) the customer's full name; and

(b) either the customer's:

(i) date of birth; or

(ii) residential address.

37.2 Where it has been determined that the money laundering or terrorism financing risk posed by the provision of a designated service to an individual is high under the assessment carried out under Section 35.1 of this Program and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information which has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

37.3 Information which is required to be verified as indicated in Section 37.1, of this Program, must be based on:

(a) reliable and independent documentation;

(b) reliable and independent electronic data; or

(c) a combination of (a) and (b) above.

38. INDIVIDUALS: VERIFICATION – PROCEDURES

38.1 The following verification procedures need to be followed for individuals:

(a) Government database verification (Section 64 of this Program);

(b) PEP verification (Section 68 of this Program);

(c) Foreign high-risk jurisdiction verification (Section 63 of this Program); and

38.2 Where it has been determined that the money laundering or terrorism financing risk posed by the provision of a designated service to an individual is medium or lower, Coin Harbour will comply with the safe harbour procedures and conduct a document identification procedure (a 'standard customer identification procedure' outlined in Sections 38.3 of this Program, should be conducted in all cases where possible).

38.3 **Standard documentation identification procedure:** The information in Section 37.1, of this Program, can be verified from an original or certified copy of a current primary photographic identification document as defined in Section 4.10 of this program.

38.4 **Non-standard customer identification procedures:** The procedures in Sections 38.5 of this Program, should only be conducted where:

(a) a 'identification procedure' in Section 38.3 of this Program, was unable to be conducted;

(b) the AML/CTF Compliance Officer forms the view that a discrepancy arose from the information collected and verified during a 'standard customer identification procedure'; or

(c) having conducted the 'standard customer identification procedure', the AML/CTF Compliance Officer is not reasonably satisfied that the customer is the individual he or she claims to be.

38.5 **Acceptable 'non-standard documentation identification procedure':** An acceptable 'non-standard domestic documentation identification procedure' would be based on:

(a) an original or certified copy of both:

(i) a current primary non-photographic identification document as defined in Section 4.9 of this program; and

(ii) a current secondary identification document as defined in Section 4.13 of this program.

38.6 In general, where Coin Harbour is asked to arrange the provision of a designated service for a customer who presents foreign based identification documentation, other than a passport, Coin Harbour will classify these clients as high risk.

38.7 When determining whether to accept non-standard foreign documentation, the AML/CTF Compliance Officer should have regard to the money laundering or terrorism financing risk posed by the provision of a designated service to a customer from that particular foreign country.

38.8 For the purposes of verification of an individual, Coin Harbour must have regard to the money laundering or terrorism financing risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Officer gives final sign-off as required in Section 69 of this Program.

39. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES

39.1 Coin Harbour does not currently provide any services to customers identified as companies. If Coin Harbour decides to provide services to companies in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 39 to 45 below.

39.2 Where a new customer is a company, either domestic or foreign, it is necessary for Coin Harbour's employee who is responsible for that customer:

(a) to identify the customer as:

(i) an individual director of a company; or

(ii) a corporate director; and

(b) to be reasonably satisfied that:

(i) the company exists; and

(ii) in respect of Beneficial Owners, Coin Harbour has complied with the requirements specified in Sections 65 and 66 of this Program.

39.3 **Information Collection:** The following KYC Information must be collected by Coin Harbour for a customer that is a company, at a minimum, in order to determine its existence:

(a) in the case of a domestic company:

(i) the full name of the company as registered by the Australian Securities and Investments Commission (**"ASIC"**);

(ii) the full address of the company's registered office;

(iii) the full address of the company's principal place of business (if any);

(iv) the ACN issued to the company;

(v) the AFSL number issued to the company (if relevant);

(vi) whether the company is registered by ASIC as a proprietary or public company; and

(vii) if the company is registered as a proprietary company, the name of each Director of the company.

(b) in the case of a registered foreign company:

(i) the full name of the company as registered by ASIC;

(ii) the full address of the company's registered office in Australia;

(iii) 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);

(iv) the ARBN issued to the company;

(v) the AFSL number issued to the company (if relevant);

(vi) the country in which the company was formed, incorporated or registered;

(vii) 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

(viii) if the company is registered as a private company by the relevant foreign registration body - the name of each Director of the company.

(c) in the case of an unregistered foreign company:

(i) the full name of the company;

(ii) the country in which the company was formed, incorporated or registered;

(iii) whether the company is registered by the relevant foreign registration body and if so:

(A) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

(B) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

(C) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

(iv) if the company is registered as a private company by the relevant foreign registration body – the name of each Director of the company; and

(v) 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.

39.4 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular company is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour will collect one or more pieces of the following information:

(a) all business names used by the company;

(b) if the company is a public company, the name of each director of the company;

(c) the nature of the business activities conducted by the company;

(d) the source of the customer's funds including the origin of funds;

(e) the nature and level of the customer's intended transaction behaviour;

(f) the name of the company secretary;

(g) the name of the Director;

(h) in the case of a foreign company:

(i) the name of the relevant foreign registration body;

(ii) any identification number issued to the company by the relevant foreign registration body;

(i) for an unlisted public company other than an Australian regulated company, the full name and address of each Beneficial Owner;

(j) 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;

(k) details of any current or recent prosecutions and inquiries related to ML, terrorist links, tax offences and corruption in respect of the company.

39.5 The AML/CTF Compliance Officer may also determine, where the money laundering or terrorism financing risk posed by the company is medium or high, that the individuals referred to in Sections 39.4(f) and 39.4(g), of this Program, must be screened against the lists mentioned in Section 64.1 of this Program.

39.6 For information collected pursuant to Sections 39.3 and 39.4 above, the verification procedures in Section 40 of this Program must also be followed, having regard to the money laundering or terrorism financing risk relevant to the provision of the designated service.

40. COMPANIES: VERIFICATION – PROCEDURES

40.1 The following verification procedures need to be followed for companies:

(a) Government database verification (refer to Section 64 of this Program); and

(b) PEP verification (refer to Section 68 of this Program); and

(c) Foreign high-risk jurisdiction verification (refer to Section 63 of this Program); and

(d) A document identification procedure (refer to Section 40.2 of this Program).

40.2 At a minimum, the following KYC Information about a customer in Section 39 of this Program must be verified:

(a) in the case of a domestic company:

(i) the full name of the company as registered by ASIC;

(ii) whether the company is registered by ASIC as a proprietary or public company; and

(iii) the ACN issued to the company;

(b) in the case of a registered foreign company:

(i) the full name of the company as registered by ASIC;

(ii) 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

(iii) the ARBN issued to the company;

(c) in the case of an unregistered foreign company:

(i) the full name of the company;

(ii) whether the company is registered by the relevant foreign registration body and if so:

(A) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration; and

(B) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body.

40.3 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular company is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour employee responsible for the customer will collect one or more pieces of the following information:

(a) in the case of a domestic company:

(i) the full address of the company's registered office;

(ii) the full address of the company's principal place of business, if any;

(iii) if the company is registered as a proprietary company, the name of each director of the company;

(b) in the case of a registered foreign company:

(i) 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;

(ii) the country in which the company was formed, incorporated or registered;

(iii) if the company is registered as a private company by the relevant foreign registration body – the name of each director of the company; and

(c) in the case of an unregistered foreign company:

(i) the country in which the company was formed, incorporated or registered;

(ii) whether the company is registered by the relevant foreign registration body and if so:

(A) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

(iii) if the company is registered as a private company by the relevant foreign registration body – the name of each director of the company; and

(iv) 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.

40.4 If the company is an unregistered foreign company, the AML/CTF Compliance Officer may determine that it is necessary to seek an explanation as to why the company is not registered.

40.5 Where it has been determined under an assessment conducted under Section 35.1, of this Program, that the money laundering or terrorism financing risk posed by the provision of a designated service to a company is medium or high and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information that has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

40.6 For information that is required to be verified as indicated in Sections 40.2 and 40.3 of this Program and, the following can be used:

(a) reliable and independent documentation (refer to Section 42 of this Program);

(b) reliable and independent electronic data (refer to Section 43 of this Program); or

(c) a combination of (a) and (b) above.

40.7 For the purposes of Section 40.6, 'reliable and independent documentation' includes a disclosure certificate that verifies information about the Beneficial Owners of a company if a reporting entity is permitted to obtain a disclosure certificate as described in Section 71 of this Program.

41. COMPANIES: SIMPLIFIED VERIFICATION PROCEDURES

41.1 The criteria in Section 40, of this Program, does not have to be satisfied where Coin Harbour confirms that the company is:

(a) a domestic listed public company;

(b) a majority owned subsidiary of a domestic listed public company; or

(c) licensed and subject to regulatory oversight of a Commonwealth, State or Territory regulator in relation to its activities as a company,

by obtaining one (1) or a combination of the following:

(d) a search of the relevant domestic stock exchange;

(e) a public document issued by the relevant company;

(f) a search of the relevant ASIC database; or

(g) a search of the licence or other records of the relevant regulator.

42. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

42.1 The following types of reliable and independent documentation are acceptable for verification of company information:

(a) an original and currently valid Australian financial services licence issued by ASIC;

(b) an original and currently valid company registration certificate issued by ASIC; or

(c) in relation to the beneficial ownership of a company, a disclosure certificate that verifies information about the beneficial ownership of a company (subject to Section 42.2 of this Program).

42.2 **Disclosure Certificates**:

(a) For a company other than a foreign company, i.e. an Australian company, a disclosure certificate will be 'reliable and independent documentation' for the purposes of this Program to verify additional information collected in respect of a company.

(b) For a foreign company where other reliable verification information is not otherwise reasonably available, a disclosure certificate verifying information about a foreign company can be relied upon by Coin Harbour for new customer KYC verification if given approval by the AML/CTF Compliance Officer. The AML/CTF Compliance Officer will take into consideration the money laundering or terrorism financing risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the company as well as 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.

43. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT ELECTRONIC DATA

43.1 When verifying KYC Information collected from a customer by means of reliable and independent electronic data, the procedures below need to be followed.

43.2 For the purposes of verification of a company other than a foreign company, the following sources are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 44.1 of this Program:

(a) ASIC (www.asic.gov.au);

(b) ASX (www.asx.com.au); and

(c) APRA (www.apra.gov.au).

43.3 For the purposes of verification of a foreign company, the following sources are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 44.1 of this Program:

(a) a search of the relevant foreign stock or equivalent exchange (if any) – refer to Section 43.4 of this Program; and

(b) a search of the records of the relevant regulator.

43.4 A relevant foreign stock or equivalent exchange is one that is approved by ASIC for recognition, including, but not limited to the following financial markets:

(a) American Stock Exchange;

(b) Borsa Italiana;

(c) Bourse de Paris;

(d) Bursa Malaysia Main Board and Bursa Malaysia Second Board;

(e) Eurex Amsterdam;

(f) Frankfurt Stock Exchange;

(g) Hong Kong Stock Exchange;

(h) JSE Securities Exchange;

(i) London Stock Exchange;

(j) NASDAQ National Market;

(k) New York Stock Exchange;

(l) New Zealand Stock Exchange;

(m) Stock Exchange of Singapore;

(n) SWX Swiss Exchange;

(o) Tokyo Stock Exchange; and

(p) Toronto Stock Exchange.

43.5 For the purposes of verification of a foreign listed public company, Coin Harbour must have regard to the money laundering or terrorism financing risk relevant to the provision of the designated services being provided (or potentially provided), including the location of the foreign stock or equivalent exchange (if any). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Officer gives final sign-off as required in Section 69 of this Program.

44. COMPANIES: VERIFICATION – ALTERNATIVE DATA

44.1 Where the data in Sections 41 and 43, of this Program, cannot be obtained or is not sufficient to verify the required data listed in Sections 39.3 and 40 of this Program, in consultation with the AML/CTF Compliance Officer, Coin Harbour's employee responsible for the customer will determine whether alternative sources of data can be obtained. This alternative data must be reliable and independent such that it can be accepted into the verification process. In making this determination, the following factors need to be taken into account:

(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 (for example, by reference to the range of persons included in the data and the period over which the data has been collected);

(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.

45. COMPANIES: VERIFICATION – INDEPENDENT CONTACT

45.1 To verify KYC Information collected from a customer, Coin Harbour's employee responsible for the customer will independently initiate contact with the company. This contact will be made using information contained in public resources such as the:

(a) White Pages Directory;

(b) Yellow Pages Directory;

(c) ASIC Database;

(d) internet searches; and

(e) APRA database.

45.2 Any of the electronic data in Sections 43.2 or 43.3, of this Program, can also be used for the purposes of this Section.

46. TRUSTS: CUSTOMER IDENTIFICATION PRINCIPLES

46.1 Coin Harbour does not currently provide any services to customers identified as trusts. If Coin Harbour decides to provide services to trusts in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 48 and 49 below.

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

(a) the trust exists (refer to Section 47 of this Program); and

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

47. TRUSTS: IDENTIFICATION PROCEDURES

47.1 In accordance with Section 46.2(a) of this Program, the following KYC Information must be collected from a customer:

(a) the full name of the trust;

(b) the full business name (if any) of the trustee in respect of the trust;

(c) the type of the trust;

(d) the country in which the trust was established;

(e) the full name of the settlor of the trust, unless:

(i) the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000.00; or

(ii) the settlor is deceased; or

(iii) the trust is verified using the simplified trustee verification procedure under Section 49 of this Program.

(f) 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 is under Sections 36 to 38 of this Program;

(g) 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 is under Sections 39 to 45 of this Program;

(h) 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 Sections 36 to 38 of this Program.

47.2 Where it is determined under an assessment carried out under Section 35.1, of this Program, that the money laundering or terrorism financing risk posed by the provision of a designated service to a trustee of a trust is medium or high, the AML/CTF Compliance Officer may require Coin Harbour's employee responsible for the customer will collect one or more pieces of the following information:

(a) all business names used by the trusts and any other name under which the trust operates;

(b) the nature of the business activities conducted by the trust;

(c) the source of the customer's funds including the origin of funds;

(d) the jurisdiction in which the trust was established;

(e) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the trust;

(f) the nature and level of the customer's intended transaction behaviour;

(g) the income and assets (including location) of the trust;

(h) details of any parties with which the trust owns property, is in partnership or undertakes a joint venture.

48. TRUSTS: VERIFICATION PROCEDURES

48.1 The following verification procedures need to be followed for trusts:

(a) Government database verification (refer to Section 64 of this Program);

(b) PEP verification (refer to Section 68 of this Program);

(c) Foreign high-risk jurisdiction verification (refer to Section 63 of this Program); and

(d) a document identification procedure (refer to Section 48.2 of this Program).

48.2 At a minimum, the following KYC Information about a customer in Section 46 of this Program must be verified:

(a) the full name of the trust from a trust deed, certified copy or certified extract of the trust deed, reliable and independent documents relating to the trust or reliable and independent electronic data;

(b) if any of the trustees is an individual, then in respect of one of those individuals – information about the individual is in accordance with the customer identification procedures in Sections 36 to 38 of this Program;

(c) if any of the trustees is a company, then in respect of one of those companies – information about the company is in accordance with the procedures in Sections 39 to 45 of this Program;

(d) if the trustees comprise individuals and companies then in respect of either an individual or a company – the information about the individual or company (as the case may be) is in accordance with the applicable procedures in Sections 36 to 45 of this Program;

(e) the full name of the settlor of the trust unless;

(i) the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000.00;

(ii) the settlor is deceased;

(iii) the trust is verified using the simplified trustee verification procedure under Section 49 of this Program.

48.3 Where it has been determined under an assessment carried out under Section 35.1, of this Program, that the money laundering or terrorism financing risk posed by the provision of a designated service to a trustee of a trust is medium or high and additional KYC Information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC Information that has been collected. The AML/CTF Compliance Officer will determine what additional KYC Information will be verified in respect of that customer.

48.4 A Disclosure Certificate will be 'reliable and independent documentation' for the purposes of Section 48.2 of this Program to verify additional information collected in respect of a trust where:

(a) the verification is for the purposes of a procedures of Section 47 of this Program; and

(b) the information is not otherwise reasonably available from the sources described in Section 48.2 of this Program.

49. TRUSTS: SIMPLIFIED VERIFICATION – PROCEDURES

49.1 The criteria in Section 47 and 51 of this Program will not need to be satisfied where it can be verified that a trustee falls into one of the following categories:

(a) a managed investment scheme registered by ASIC;

(b) a managed investment scheme that is not registered by ASIC and that:

(i) only has wholesale customers; and

(ii) does not make small scale offerings to which section 1012E of the *Corporations Act* 2001 (Cth) applies;

(c) registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or

(d) a government superannuation fund established by legislation.

50. TRUSTEES AND BENEFICIARIES: IDENTIFICATION PROCEDURES

50.1 Coin Harbour does not currently provide any services to customers identified as trustees and/or beneficiaries. If Coin Harbour decides to provide services to trustees and/or beneficiaries in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 50 and 51 below.

50.2 In accordance with Section 46.2(b) of this Program, the following KYC Information must be collected from a customer:

(a) the full name and address of each trustee in respect of the trust; and

(b) either the:

(i) full name of each beneficiary of the trust; or

(ii) if the terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.

51. TRUSTEES AND BENEFICIARIES: VERIFICATION PROCEDURES

51.1 The information collected under Section 49 of this Program must be verified by:

(a) a trust deed, certified copy or certified extract of a trust deed;

(b) reliable and independent documents relating to the trust;

(c) reliable and independent electronic data; or

(d) a combination of (a) to (c) above.

51.2 For the purposes of Sections 51.1(b) and 51.1(c) of this Program, 'reliable and independent documents relating to the trust' includes a disclosure certificate that verifies information about a trust where:

(a) the verification is being conducted as a result of a risk-based assessment in Section 32.2(b) of this Program determining that additional information is required about the trustee; and

(b) the information to be verified is not otherwise reasonably available from the sources in Section 51.1 of this Program.

51.3 For the purposes of verification of a trustee, Coin Harbour must have regard to the money laundering or terrorism financing risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Officer gives final sign-off as required in Section 69 of this Program.

52. PARTNERSHIPS: CUSTOMER IDENTIFICATION PROCEDURES

52.1 Coin Harbour does not currently provide any services to customers identified as partnerships. If Coin Harbour decides to provide services to partnerships in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 52 and 53 below.

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

(a) the partnership exists; and

(b) the name of each of the partners in the partnership has been provided in accordance with Section 52.3(e).

52.3 The following KYC Information must be collected by Coin Harbour for a customer that is a partnership, at a minimum:

(a) full name of the partnership;

(b) the full business name (if any) of the partnership as registered under any State or Territory business names legislation

(c) the country in which the partnership was established;

(d) in respect of one of the partners – the information required to be collected under Section 36; and

(e) 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

52.4 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular partnership is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour's employee to be responsible for the customer. One or more of the following pieces of information will be collected:

(a) any alias names used by the partner;

(b) the partnership's business activities;

(c) the source of the partnership's funds including the origin of funds;

(d) income and assets of the partnership;

(e) the nature and level of the partnership's intended transaction behaviour; and

(f) the beneficial ownership of the funds used by the partnership/the partnership's account with Coin Harbour.

52.5 The information collection requirements in this Section are not intended to conflict with any other obligation Coin Harbour has under other legislation including the *Privacy Act* 1988. Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

53. PARTNERSHIPS: VERIFICATION – PRINCIPLES

53.1 At a minimum, the following KYC Information about a customer in Section 52 of this Program, must be verified:

(a) the full name of the partnership from the partnership agreement, certified copy or certified extract of the partnership agreement, reliable and independent documents relating to the partnership or reliable and independent electronic data;

(b) information about one of the partners in accordance with the applicable customer identification procedure with respect to individuals set Section 36.

53.2 Information which is required to be verified as indicated in Section 53.1 of this Program, must be based on:

(a) a partnership agreement, certified copy or certified extract of a partnership agreement;

(b) a certified copy or certified extract of minutes of a partnership meeting;

(c) reliable and independent documentation;

(d) reliable and independent electronic data; or

(e) a combination of (a) to (d) above.

53.3 For the purposes of Section 53.2 'reliable and independent documentation' includes a disclosure certificate that verifies information about the Beneficial Owners of a company if a reporting entity is permitted to obtain a disclosure certificate as described in Section 71 of this Program.

54. ASSOCIATIONS: CUSTOMER IDENTIFICATION PROCEDURES

54.1 Coin Harbour does not currently provide any services to customers identified as associations. If Coin Harbour decides to provide services to associations in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 54 and 55 below.

54.2 Where a new customer is an incorporated or unincorporated association, it is necessary for Coin Harbour to be reasonably satisfied that:

(a) the association exists; and

(b) the names of any members of the governing committee (howsoever described) of the association have been provided.

54.3 The following KYC Information must be collected by Coin Harbour for a customer that is an incorporated association, at a minimum:

(a) the full name of the association;

(b) 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;

(c) 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

(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association.

54.4 The following KYC Information must be collected by Coin Harbour's employee who is responsible for a customer that is a member of an unincorporated association, at a minimum:

(a) the full name of the association;

(b) the full address of the association's principal place of administration (if any);

(c) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and

(d) in respect of the member – the information required to be collected from an individual under the applicable customer identification procedure with respect to individuals set out in an AML/CTF program.

54.5 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular association is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour's employee to be responsible for the customer. One or more of the following pieces of information will be collected:

(a) any alias names used by the member of the association;

(b) the association's business activities;

(c) the source of the association's funds including the origin of funds;

(d) income and assets of the association;

(e) the nature and level of the association's intended transaction behaviour; and

(f) the beneficial ownership of the funds used by the member/the association's account with Coin Harbour.

54.6 The information collection requirements in this Section are not intended to conflict with any other obligation Coin Harbour has under other legislation including the *Privacy Act* 1988*.* Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

55. ASSOCIATIONS: VERIFICATION – PRINCIPLES

55.1 At a minimum, the following KYC Information about a customer who is an incorporated association, must be verified:

(a) the full name of the incorporated association; and

(b) any unique identifying number issued to the incorporated association upon its incorporation;

from information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association or from the rules or constitution of

the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data:.

55.2 At a minimum, the following KYC Information about a customer who is an unincorporated association, must be verified:

(a) the full name (if any) of the association from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data; and

(b) information about the member in accordance with the applicable customer identification procedure with respect to individuals set out in Section 35.

55.3 Information which is required to be verified as indicated in Section 55.1 of this Program, must be based on:

(a) the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;

(b) the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association;

(c) 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;

(d) reliable and independent documentation;

(e) reliable and independent electronic data; or

(f) a combination of (a) to (e) above.

55.4 For the purposes of Section 55.3 ‘reliable and independent documentation’ includes a disclosure certificate that verifies information about the Beneficial Owners of a company if a reporting entity is permitted to obtain a disclosure certificate as described in Section 71 of this Program.

56. REGISTERED COOPERATIVES: CUSTOMER IDENTIFICATION PROCEDURES

56.1 Coin Harbour does not currently provide any services to customers identified as registered cooperatives. If Coin Harbour decides to provide services to registered cooperatives in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 56 and 57 below.

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

(a) the co-operative exists; and

(b) the names of the chairman, secretary or equivalent in each case of the co-operative have been provided.

56.3 The following KYC Information must be collected by Coin Harbour for a customer that is a registered co-operative, at a minimum:

(a) the full name of the co-operative;

(b) 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;

(c) 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

(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative.

56.4 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular association is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour's employee to be responsible for the customer. One or more of the following pieces of information will be collected:

(a) any alias names used by the member of the co-operative;

(b) the co-operative's business activities;

(c) the source of the co-operative's funds including the origin of funds;

(d) income and assets of the co-operative;

(e) the nature and level of the co-operative's intended transaction behaviour; and

(f) the beneficial ownership of the funds used by the member/the co-operative's account with Coin Harbour.

56.5 The information collection requirements in this Section are not intended to conflict with any other obligation Coin Harbour has under other legislation including the *Privacy Act* 1988*.* Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

57. REGISTERED COOPERATIVES: VERIFICATION – PRINCIPLES

57.1 At a minimum, the following KYC Information about a customer who is an incorporated association, must be verified:

(a) the full name of the co-operative; and

(b) any unique identifying number issued to the co-operative upon its incorporation;

from information provided by ASIC or by the State, Territory or overseas body responsible for the registration of the co-operative or from any register maintained by the co-operative or from a certified copy or certified extract of any register maintained by the co-operative or from reliable and independent documents relating to the co-operative or from reliable and independent electronic data.

57.2 Information which is required to be verified as indicated in Section 57.1 of this Program, must be based on:

(a) any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative;

(b) the minutes of meeting of the co-operative or a certified copy or certified extract of minutes of meeting of the co-operative;

(c) information provided by the State, Territory or overseas body responsible for the registration of the co-operative;

(d) reliable and independent documentation;

(e) reliable and independent electronic data; or

(f) a combination of (a) to (e) above.

57.3 For the purposes of Section 57.2 'reliable and independent documentation' includes a disclosure certificate that verifies information about the Beneficial Owners of a company if a reporting entity is permitted to obtain a disclosure certificate as described in Section 71 of this Program.

58. GOVERNMENT BODIES: CUSTOMER IDENTIFICATION PROCEDURES

58.1 Coin Harbour does not currently provide any services to customers identified as government bodies. If Coin Harbour decides to provide any services to government bodies in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 58 and 59 below.

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

(a) the government body exists; and

(b) in the case of certain kinds of government bodies – information about the beneficial owners of the government body.

58.3 The following KYC Information must be collected by Coin Harbour for a customer that is a government body, at a minimum:

(a) the full name of the government body;

(b) the full address of the government body's principal place of operations;

(c) whether the government body is an entity or emanation, or is established under legislation, of the Commonwealth; and

(d) whether the government body is an entity or emanation, or is established under legislation, of a State, Territory, or a foreign country and the name of that State, Territory or country.

58.4 Where the money laundering or terrorism financing risk posed by the provision of a designated service to a particular government body is assessed as medium or high under Section 35.1 of this Program, the AML/CTF Compliance Officer may require Coin Harbour's employee to be responsible for the customer. One or more of the following pieces of information will be collected:

(a) any alias names used by the member of the government body;

(b) the government body's business activities;

(c) the source of the government body's funds including the origin of funds;

(d) income and assets of the government body;

(e) the nature and level of the government body's intended transaction behaviour; and

(f) the beneficial ownership of the funds used by the member/the government body's account with Coin Harbour.

58.5 The information collection requirements in this Section are not intended to conflict with any other obligation Coin Harbour has under other legislation including the *Privacy Act* 1988. Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

59. GOVERNMENT BODIES: VERIFICATION – PRINCIPLES

59.1 At a minimum, the following KYC Information about a customer who is a government body, must be verified:

(a) the full name of the government body;

(b) the full address of the government body's principal place of operations;

(c) whether the government body is an entity or emanation, or is established under legislation, of the Commonwealth; and

(d) whether the government body is an entity or emanation, or is established under legislation, of a State, Territory, or a foreign country and the name of that State, Territory or country.

59.2 Information which is required to be verified as indicated in Section 59.1 of this Program, must be based on:

(a) reliable and independent documentation;

(b) reliable and independent electronic data; or

(c) a combination of (a) and (b) above.

60. AGENTS: IDENTIFICATION PROCEDURES

60.1 Coin Harbour currently does not provide any services to an agent who requests the provision of a designated service on behalf of a customer. If Coin Harbour decides to provide any services to agents in the future, Coin Harbour will carry out the due diligence measures in accordance with Sections 60 and 61.

60.2 Where an agent requests the provision of a designated service on behalf of a customer, Coin Harbour must collect, at a minimum the following:

(a) the full name of each individual who purports to act for or on behalf of the customer with respect to the provision of a designated service by Coin Harbour; and

(b) evidence of the customer's authorisation of any individual to act on its behalf.

60.3 Where an agent requests the provision of a designated service on behalf of a customer, Coin Harbour will carry out the relevant customer identification procedure outlined in Part B of this Program, in respect of that customer.

61. AGENTS: VERIFICATION PRINCIPLES

61.1 Coin Harbour will not verify the identity of the agent where the money laundering or terrorism financing risk associated with the provision of a designated service is classified as low by the AML/CTF Compliance Officer.

61.2 Where it is determined that the money laundering or terrorism financing risk associated with the provision of a designated service to the particular customer is medium or high, Coin Harbour will verify the information specified in Section 60.2 of this Program, in accordance with the requirements of Section 37.3 of this Program.

61.3 Coin Harbour will verify the identity of the customer in accordance with its customer identification procedures set out in Part B of this Program.

62. VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

62.1 It is assumed that any document used to verify KYC Information will be sufficiently contemporaneous unless otherwise specified in the AML/CTF Rules or in this Program. For the purposes of this Program, a document will be sufficiently contemporaneous if it has not expired or, where it does not have an expiry date, is no more than three (3) months old.

62.2 If a customer is unable to provide an original copy of a document for the purposes of verifying KYC Information, the AML/CTF Compliance Officer will need to determine, having regard to the money laundering or terrorism financing risk associated with the provision of a designated service to that customer, whether it is appropriate to rely on a certified copy of the document.

62.3 The AML/CTF Compliance Officer will take steps to determine whether any document produced by a customer has been forged, tampered with, cancelled or stolen.

63. VERIFICATION – FOREIGN JURISDICTIONS

63.1 Where Coin Harbour has the prospect to acquire a new customer from a foreign jurisdiction, an assessment must be made as to whether it is a high-risk jurisdiction. The factors that should be considered in this assessment include, but are not limited to:

(a) whether the customer is based in a country that is a Financial Action Task Force (**"FATF"**) member and any FATF reports about that country;

(b) the legal framework and standard AML/CTF controls of the foreign jurisdiction; and

(c) the economic climate of the foreign jurisdiction.

63.2 The assessment should take into account information from legitimate, respected domestic and/or international bodies.

63.3 Where an assessment is made that the customer is from a high-risk jurisdiction, the matter must be referred to the AML/CTF Compliance Officer who will make a decision as to whether Coin Harbour should continue dealing with the customer.

64. VERIFICATION – GOVERNMENT DATABASES

64.1 Where Coin Harbour is likely to provide designated services to a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in this Program by Coin Harbour:

(a) Department of Foreign Affairs and Trade's (**"DFAT"**) Consolidated List:

(i) the name of a prospective customer must be checked against the DFAT Consolidated List available at http://dfat.gov.au/international-relations/security/sanctions/pages/consolidated-list.aspx;

(ii) the DFAT Consolidated List must be accessed directly from the DFAT website every time a prospective customer is checked – a copy of this spreadsheet should not be saved on an employee's computer in order to ensure that the most recent version of the Consolidated List is used;

(iii) alternatively, the DFAT 'LinkMatch Lite' software may be used to check the names of a prospective customer – prior to a prospective customer being checked, the most recent version of the 'LinkMatch Lite' software can be obtained by emailing your request to DFAT at asset.freezing@dfat.gov.au. For more information, please refer to the section "LinkMatchLite" at http://dfat.gov.au/international-relations/security/sanctions/pages/consolidated-list.aspx#list;

(iv) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer who will report to Australian Federal Police ("**AFP**");

(v) where a match is found on the DFAT Consolidated List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer. For more information, please refer to the section "Reporting to the Australian Federal Police" at http://dfat.gov.au/international-relations/security/sanctions/pages/consolidated-list.aspx#list; and

(vi) if it is unclear whether there is a match between the name provided and any name on the Consolidated List, the AML/CTF Compliance Officer must be immediately notified and Coin Harbour may request the assistance of the AFP to confirm/advise on the match. For more information, please refer to the section "Australian Federal Police assistance to find a match" at http://dfat.gov.au/international-relations/security/sanctions/pages/consolidated-list.aspx#list.

(b) Australian National Security (**"ANS"**):

(i) the name of the new customer must be checked against the ANS Listing of Terrorist Organisations available at http://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/default.aspx;

(ii) the ANS Listing of Terrorist Organisations must be accessed directly from the ANS website listed in Section 64.1(b)(i) of this Program every time a prospective customer is being checked – a copy of this list should not be saved on an employee's computer in order to ensure that the most recent version is used;

(iii) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer; and

(iv) where there is a match with the ANS Listing of Terrorist Organisations, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer.

(c) Criminal Code List:

(i) the name of a new customer must be checked against the list contained in the *Criminal Code Regulations* 2002 available at: https://www.legislation.gov.au/;

(ii) where there is a match it must be **immediately** referred to the AML/CTF Compliance Officer; and

(iii) where there is a match with the Criminal Code List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Officer.

65. BENEFICIAL OWNERS: IDENTIFICATION PROCEDURES

65.1 For definition of "Beneficial Owner", please see Section 4 of this Program.

Determining the Beneficial Owner of each customer

65.2 If during the KYC procedures under Section 39 of this Program it is not immediately apparent who the Beneficial Owners of a customer are, Coin Harbour's must identify all that customer's Beneficial Owners before providing a designated service to that customer or enter into a business relationship with them.

65.3 In identifying the Beneficial Owners of a customer, Coin Harbour may:

(a) collect from the customer information relating to the ownership structure of the customer including but not limited to:

(i) information relating to the shareholders of the company;

(ii) information relating to the people exercising responsibility for senior management decisions, or similar, of the customer;

(iii) information relating to the people with the ability to control the customer and/or dismiss or appoint those in senior management positions;

(iv) information relating to those people holding more than 25% of the customer's rights;

(v) information relating to those individuals (for example, the CEO) who hold senior management positions; and

(vi) 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 Coin Harbour has a clear understanding of who the ultimate Beneficial Owners of the customer are.

65.4 Coin Harbour must take reasonable measures to collect and verify:

(a) each Beneficial Owner's full name, and

(b) the Beneficial Owner's date of birth; or

(c) the Beneficial Owner's full residential address.

65.5 The steps in Section 65.4 must be carried out by Coin Harbour either before the provision of designated service to the customer or as soon as practicable after the designated service has been provided.

65.6 The steps in Section 65.4 do not need to be carried out for a customer who is:

(a) an individual. Coin Harbour may assume that the customer and the Beneficial Owner are one and the same, unless Coin Harbour has reasonable grounds to consider otherwise;

(b) a company which is verified under the simplified company verification procedure under Section 41 of this Program;

(c) a trust which is verified under the simplified trustee verification procedure under Section 49 of this Program;

(d) an Australian Government Entity; or

(e) a foreign listed public company, or a majority-owned subsidiary of such a company subject to disclosure requirements (whether by stock exchange rules or by law or enforceable means) that ensure transparency of beneficial ownership.

65.7 The AML/CTF Compliance Officer will determine whether any additional information in addition to the information referred to in Section 65.4 will be collected and verified from a customer about any Beneficial Owner.

66. BENEFICIAL OWNERS: VERIFICATION PROCEDURES

66.1 Information which is required to be verified as indicated in Section 65.4, of this Program, must be based on:

(a) reliable and independent documentation;

(b) reliable and independent electronic data; or

(c) a combination of (a) and (b) above.

66.2 Where it has been determined that the money laundering or terrorism financing risk posed by the provision of a designated service to an individual and Beneficial Owner is medium or lower, Coin Harbour will comply with the safe harbour procedures and conduct a document

identification procedure (a 'standard customer identification procedure' outlined in Sections 66.3 of this Program, should be conducted in all cases where possible).

66.3 **Standard documentation identification procedure:** The information in Section 65.4 of this Program can be verified from an original or certified copy of a current primary photographic identification document as defined in Section 4.10 of this program.

66.4 **Non-standard documentation identification procedures:** The procedures in Sections 66.5 of this Program, should only be conducted where:

(a) an 'identification procedure' in Sections 66.3 of this Program was unable to be conducted;

(b) the AML/CTF Compliance Officer forms the view that a discrepancy arose from the information collected and verified during a 'standard documentation identification procedure'; or

(c) having conducted the 'standard documentation identification procedure', the AML/CTF Compliance Officer is not reasonably satisfied that the customer is the individual he or she claims to be.

66.5 **Acceptable 'non-standard documentation identification procedure':** An acceptable 'non-standard domestic documentation identification procedure' would be based on:

(a) an original or certified copy of both:

(i) a current primary non-photographic identification document as defined in Section 4.9 of this program; and

(ii) a current secondary identification document as defined in Section 4.13 of this program.

66.6 When determining whether to accept non-standard foreign documentation, the AML/CTF Compliance Officer should have regard to the money laundering or terrorism financing risk posed by the provision of a designated service to a customer from that particular foreign country.

66.7 For the purposes of verification of an individual, Coin Harbour must have regard to the money laundering or terrorism financing risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Officer gives final sign-off as required in Section 69 of this Program.

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

66.9 The AML/CTF Compliance Officer must then collect from the customer whatever additional information they consider necessary to verify that the Beneficial Owner is the person that the customer claim they are.

67. PROCEDURE TO FOLLOW WHERE UNABLE TO DETERMINE THE IDENTITY OF THE BENEFICIAL OWNER

67.1 If Coin Harbour 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 which is verified under the simplified company verification procedure under Section 41 of this Program) or a partnership, any individual who:

(i) is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including power to veto, or

(ii) holds the position of senior managing official (or equivalent);

(b) for a trust (other than a trust which is verified under the simplified trustee verification procedure under Section 49 of this Program), 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:

(i) is entitled (either directly or indirectly) to exercise 25% or more of the voting rights including a power of veto, or

(ii) would be entitled on dissolution to 25% or more of the property of the association or registered co-operative, or

(iii) holds the position of senior managing official (or equivalent).

68. PEP: IDENTIFICATION AND VERIFICATION PROCEDURES

68.1 See the Definitions section of this Program for the definitions of various PEPs.

68.2 If when conducting the risk analysis in Section 11 of this Program, Coin Harbour has a reasonable suspicion that a customer is a politically exposed person (PEP), the AML/CTF Compliance Officer, 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:

(a) a customer self-declaration regarding their PEP status;

(b) an internet and media search;

(c) a search of relevant commercial databases (if available to Coin Harbour;

(d) Government issued PEP lists relevant to the jurisdiction/s of the customer;

(e) Information sharing databases relating to PEP within the Australian financial system; and

(f) asset disclosure systems.

68.3 If Coin Harbour determines that a customer is a domestic PEP or an international organisation PEP, it must carry out the following procedures in relation to that customer:

(a) in the case of a Beneficial Owner, comply with the identification requirements specified in Section 36 of this Program as if the PEP was the customer;

(b) determine whether the customer is of high money laundering or terrorism financing risk; and

(c) if the customer is determined to be of high money laundering or terrorism financing risk, then, in addition to the action specified in Section 68.3(a), carry out the actions in Sections 68.4(b) - 68.4(c) below.

68.4 If Coin Harbour determines that a customer is a foreign PEP, it must carry out the following procedures in relation to that customer:

(a) in the case of a Beneficial Owner, comply with the identification requirements specified in Section 36 of this Program as if the PEP was a customer; and

(b) obtain the Board of Directors' 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;

(c) take reasonable measures to establish the politically exposed person's source of wealth and source of funds; and

(d) comply with the ongoing due diligence obligations as per Section 25 of this Program.

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

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

69. NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF COMPLIANCE OFFICER

69.1 The AML/CTF Compliance Officer must be notified of all new customers prior to the provision of any services.

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

70. TOLERANCE OF DISCREPANCIES AND ERRORS

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

70.2 **Pre-defined tolerance levels for matches and errors:** Coin Harbour 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 Compliance Officer should be notified and independent contact should be initiated with the customer to clarify the information.

71. DISCLOSURE CERTIFICATES

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

(a) Coin Harbour 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) Coin Harbour 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 on or more of the items of information specified in Sections 71.2 - 71.8 below.

Domestic Companies

71.2 For the purposes of Section 40.7, a disclosure certificate for a domestic company must contain:

(a) the full name and full residential address of each beneficial owner of the company;

(b) the full name of the appropriate officer;

(c) a certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate and complete; to the best of their knowledge and belief; and

(d) the date of certification by the appropriate officer.

Foreign companies

71.3 For the purposes of Sections 42.1 and 42.2, a disclosure certificate for a foreign company registered in Australia must contain:

(a) the full name of the company;

(b) information about 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;

(c) the full name and full residential address of each beneficial owner;

(d) the full name of the appropriate officer;

(e) certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate, and complete, to the best of their knowledge and belief; and

(f) the date of certification by the appropriate officer.

71.4 For a foreign company not registered in Australia a disclosure certificate must contain:

(a) the full name of the company;

(b) information about whether the company is registered by the relevant foreign registration body and if so:

(i) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

(ii) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

(iii) the jurisdiction of incorporation of the foreign company as well as the jurisdiction of the primary operations of the foreign company and the location of the foreign stock or equivalent exchange (if any); and

(iv) contain the full name and full residential address of each beneficial owner;

(c) the full name of the appropriate officer;

(d) certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate, and complete, to the best of their knowledge and belief; and

(e) the date of certification by the appropriate officer.

Trusts

71.5 For the purposes of Section 48.4, a disclosure certificate for a trust must:

(a) verify KYC information about a trust;

(b) contain the full name and full residential address of each beneficial owner;

(c) contain the full name of the appropriate officer;

(d) contain certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate and complete; to the best of their knowledge and belief; and

(e) contain the date of certification by the appropriate officer.

Partnerships

71.6 For the purposes of Section 53.3, a disclosure certificate for a partnership must:

(a) verify KYC information about a partnership;

(b) contain the full name and full residential address of each beneficial owner;

(c) contain the full name of the appropriate officer;

(d) contain certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate, and complete, to the best of their knowledge and belief; and

(e) contain the date of certification by the appropriate officer.

Associations

71.7 For the purposes of Section 55.4, a disclosure certificate for an incorporated or unincorporated association must:

(a) verify KYC information about an association;

(b) contain the full name and full residential address of each beneficial owner;

(c) contain the full name of the appropriate officer;

(d) contain certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate, and complete; to the best of their knowledge and belief; and

(e) contain the date of certification by the appropriate officer.

Registered Co-operatives

71.8 For the purposes of Section 57.3, a disclosure certificate for an incorporated or unincorporated association must:

(a) verify KYC information about a registered co-operative;

(b) contain the full name and full residential address of each beneficial owner;

(c) contain the full name of the appropriate officer;

(d) contain certification by the appropriate officer that the information contained in the disclosure certificate is true, accurate, and complete, to the best of their knowledge and belief; and

(e) contain the date of certification by the appropriate officer.

Issued by the Board of Directors of Coin Harbour

6-June-2021

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 1993;

(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 1993. 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 – SK ASSESSMENT AND MANAGEMENT MATRIX

See attached.