

Anti-Money Laundering and Counter-Terrorism Financing Program

Shinyuan International Pty Ltd

ACN: 639 748 306

Version Control Table

Effective Date:	25 April 2020
Date Prepared:	<u>22 April 2020</u>
Date Approved:	25 April 2020
Version No.:	1
Drafted by:	Innoinvest FS Pty Ltd
Approved by:	Shinyuan International Pty Ltd
Signature:	

INNOINVEST
Australian Financial Services Advisors

Level 11 / 20 Hunter St
Sydney NSW 2000
T 02 9247 0022

CONTENTS

1.	OVERVIEW	4
2.	ABOUT THE AML/CTF ACT	4
3.	SUMMARY OF GENERAL OBLIGATIONS	5
4.	DEFINITIONS	5
5.	DESIGNATED BUSINESS GROUP.....	5
6.	RECORDS RELATING TO THIS AML/CTF PROGRAM.....	6
7.	AML/CTF REPORTING	7
PART A.....	7
8.	INTRODUCTION.....	7
9.	ANALYSIS OF DESIGNATED SERVICES AND ML/TF RISK	7
10.	APPLICATION OF PART A.....	11
11.	THE AML/CTF COMPLIANCE OFFICER	11
12.	EMPLOYEE DUE DILIGENCE PROGRAM.....	12
13.	RISK AWARENESS TRAINING PROGRAM.....	14
14.	OUTSOURCING.....	15
15.	PROVISION OF DESIGNATED SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES.....	16
16.	RECORD KEEPING OBLIGATIONS RELATING TO CUSTOMER IDENTIFICATION AND THE PROVISION OF DESIGNATED SERVICES	16
17.	SUSPICIOUS MATTER REPORTING	17
18.	REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER.....	19
19.	ONGOING CUSTOMER DUE DILIGENCE – OVERVIEW	20
20.	ADDITIONAL KYC INFORMATION.....	21
21.	TRANSACTION MONITORING PROGRAM	22
22.	ENHANCED CUSTOMER DUE DILIGENCE PROGRAM	23
23.	REVIEW OF THE AML/CTF PROGRAM.....	25

24.	AUSTRAC FEEDBACK	30
25.	OVERSIGHT BY THE MANAGING DIRECTOR / UPDATING THE PROGRAM 30	
26.	REPORTS TO BE LODGED WITH AUSTRAC	31
PART B – CUSTOMER IDENTIFICATION		33
27.	INTRODUCTION	33
28.	APPLICATION OF PART B	33
29.	KYC – CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES 33	
30.	KNOW YOUR CUSTOMER – CONSIDERATIONS	34
31.	INDIVIDUALS: CUSTOMER IDENTIFICATION PROCEDURES	35
32.	INDIVIDUALS: VERIFICATION – PRINCIPLES	36
33.	INDIVIDUALS: VERIFICATION – PROCEDURES	37
34.	COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES	40
35.	COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES – BENEFICIAL OWNERS	42
36.	COMPANIES: VERIFICATION – PROCEDURES	43
37.	COMPANIES: SIMPLIFIED VERIFICATION PROCEDURES	45
38.	COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION	45
39.	COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT ELECTRONIC DATA	46
40.	COMPANIES: VERIFICATION – ALTERNATIVE DATA	47
41.	COMPANIES: VERIFICATION – INDEPENDENT CONTACT	48
42.	TRUSTEES: CUSTOMER IDENTIFICATION PRINCIPLES	48
43.	EXISTENCE OF THE TRUST – CUSTOMER IDENTIFICATION PROCEDURES	48
44.	EXISTENCE OF THE TRUST – VERIFICATION – PROCEDURES	49
45.	TRUSTEES AND BENEFICIARIES – CUSTOMER IDENTIFICATION PROCEDURES	50
46.	TRUSTEES AND BENEFICIARIES – VERIFICATION – PROCEDURES	51

47.	TRUSTEES: SIMPLIFIED VERIFICATION – PROCEDURES.....	51
48.	AGENTS: IDENTIFICATION PROCEDURES.....	52
49.	AGENTS: VERIFICATION PRINCIPLES.....	52
50.	VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION.....	52
51.	VERIFICATION – FOREIGN JURISDICTIONS.....	53
52.	IDENTIFICATION AND VERIFICATION – BENEFICIAL OWNERS.....	53
53.	IDENTIFICATION AND VERIFICATION – POLITICALLY EXPOSED PERSON ('PEP')	54
54.	NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF COMPLIANCE OFFICER.....	55
55.	TOLERANCE OF DISCREPANCIES AND ERRORS	55
56.	COMPLIANCE OFFICER TO SIGN.....	56
	ANNEXURE A	57

1. OVERVIEW

- 1.1. The *Anti-Money Laundering and Counter-Terrorism Financing 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 (“**ML**”) and Terrorism Financing (“**TF**”) 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. ML 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. TF is the use of money, which may or may not be generated from criminal activity, for financing terrorist activities.
- 1.4. Shinyuan International Pty Ltd (ACN 639 748 306) (“**Shinyuan**”) is a corporation established for the purpose of providing remittance services.
- 1.5. The remittance sector is recognised by Australian law enforcement and national security authorities as being vulnerable to targeting by criminals for ML/TF and the financing of serious and transnational crime, including people smuggling.
- 1.6. Shinyuan has implemented this AML/CTF Program (“**Program**”) in accordance with its risk-based approach to ML/TF risk associated with the remittance sector. This Program will ensure as far as is reasonably possible that:
 - (a) Shinyuan’s staff are adequately trained and aware of ML/TF risk associated with remittance;
 - (b) Shinyuan’s services are not used for illegitimate and illegal ends; and
 - (c) Shinyuan remains compliant with the spirit and provisions of Australian law.

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. 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 ML and TF 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 program in place to identify, mitigate and manage the risk of their products or services being used to facilitate ML or TF.

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; and
- c) have an AML/CTF Compliance Officer.

3.2. Reporting entities must also:

- a) report suspicious matters to AUSTRAC's Chief Executive Officer ("CEO"); and
- b) 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 the AML/CTF Program of Shinyuan, unless otherwise specified.

5. DESIGNATED BUSINESS GROUP

5.1. Shinyuan (a **Reporting Entity** ("RE")) does not currently share obligations with another person, for the purposes of forming a Designated Business Group ("DBG") under the AML/CTF Act and Rules.

5.2. Another entity can join with Shinyuan to form Shinyuan's DBG if:

(a) that entity is:

- (i) related to each other member of Shinyuan's DBG within the meaning of section 50 of the *Corporations Act 2001* (Cth);

either:

(A) a RE;

(B) a company in a foreign country which if it were resident in Australia would be a RE; or

- (ii) providing a designated service pursuant to a joint venture agreement, to which each member of Shinyuan's DBG is a party; and

(iii) not a member of another DBG; or

(b) otherwise permitted by the AML/CTF Act or Rules.

5.3. In order to join Shinyuan's DBG, a director or officer of the other entity will need to elect in writing (on behalf of that entity) to be a member of Shinyuan's DBG by completing the election form as specified by AUSTRAC at the time. The AML/CTF Compliance Officer will provide the

completed form to AUSTRAC in the method specified by AUSTRAC.

- 5.4. When any of the following changes in Shinyuan's DBG occurs, the AML/CTF Compliance Officer must notify AUSTRAC's CEO, in writing, by completing the approved notification form:
 - (a) a withdrawal of a member from Shinyuan's DBG;
 - (b) an election of a new member to join Shinyuan's DBG;
 - (c) the termination of Shinyuan's DBG; or
 - (d) any other change in the details previously notified to AUSTRAC's CEO in respect of the Nominated Contact Officer or Shinyuan's DBG.
- 5.5. Any of the changes listed in Section 5.4 of this Program must be approved by the Board of Directors of Shinyuan's DBG.
- 5.6. The AML/CTF Compliance Officer must provide the notification to AUSTRAC no later than fourteen (14) days. The AML/CTF Compliance Officer, must be tabled at the next meeting of the Internal Compliance Committee held after the report is completed.
- 5.7. In addition, this policy will be reviewed following any substantive changes to AML/CTF legislation or external factors such as regulatory feedback.
- 5.8. This policy will also be reviewed following any substantive changes in the perceived ML/TF risk of jurisdictions by a domestic or international institution.

6. RECORDS RELATING TO THIS AML/CTF PROGRAM

- 6.1. The AML/CTF Compliance Officer will ensure that the following records are retained for each of Shinyuan's DBG reporting entities:
 - (a) this Policy, Shinyuan's AML/CTF Program and each variation to them;
 - (b) Board of Directors' approval of this Policy, Shinyuan's AML/CTF Program and each variation to them;
 - (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 7.1 of this Policy will be retained:
 - (a) in the case of records relating to the adoption of each variation to this Policy and Shinyuan's AML/CTF 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. AML/CTF REPORTING

- 7.1. The reporting obligations that apply to Shinyuan and its AML/CTF functions, under the relevant sections of the AML/CTF Act, are:
- (a) Reports of suspicious matters;
 - (b) AML/CTF Compliance Reports.

PART A

8. INTRODUCTION

- 8.1. Part A of this Program is designed to identify, mitigate and manage the risk which Shinyuan 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 ML or TF.
- 8.2. Shinyuan should use this Program to understand the nature and purpose of its business relationships with customers. This includes:
- (a) Collecting information relevant to that understanding;
 - (b) Understanding the control structure of non-individual customers;
 - (c) Identifying significant changes in ML/TF risk;
 - (d) Identifying, mitigating and managing the ML/TF risk posed by:
 - (i) All new designated services prior to introducing them;
 - (ii) All new methods of delivering a designated service 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 all existing customers.

9. ANALYSIS OF DESIGNATED SERVICES AND ML/TF RISK

- 9.1. In determining and putting in place appropriate risk-based systems and controls to identify, mitigate and manage ML/TF risks in Part A of this Program, Shinyuan has had regard to the following factors:
- (a) The nature, size and complexity of its business; and
 - (b) The type of ML/TF risk that it might reasonably face.
- 9.2. Shinyuan has also considered the following factors when identifying Shinyuan's exposure to ML and TF, the:
- (a) types of customers it deals with;

- (b) its 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) types of designated services provided;
- (f) the methods by which those designated services are delivered; and
- (g) the foreign jurisdictions with which it operates in.

9.3. Shinyuan provides the following designated services:

- (a) Item 31 of Table 1 of section 6 of the AML/CTF Act (in the capacity of a non-financier carrying on the business of giving effect to remittance arrangements, accepting an instruction from a transferor entity for the transfer of money or property under a designated remittance arrangement);

9.4. In order to appropriately consider, identify, manage and mitigate all ML/TF risks, the risks posed by different designated services must be accounted for in the following manner:

- (a) The ML/TF risk posed by an individual customer must be considered, having regard to the particular characteristics of the individual customer, the nature, size and complexity of Shinyuan's business, and the type of ML/TF risks Shinyuan might face, including the following factors:
 - (i) The remittance services provided by Shinyuan can involve large sums of money;
 - (ii) Shinyuan's remittance services appeal to a very wide range of customers with various backgrounds and deal with a large range of jurisdictions
 - (iii) Shinyuan's wide range of customers, and large customer base, has the potential to attract problems associated with verifying identity;
 - (iv) The projects that Shinyuan provides services for are locally based;
 - (v) The item listed in Section 9.3 might have particular appeal to PEPs.
- (b) Risks are to be managed and mitigated through the following procedures:
 - (i) Shinyuan will not provide a designated service that has the capacity to directly enable customer to launder money or finance terrorism;
 - (ii) Shinyuan will continuously monitor FATF and take all necessary risk-based procedures including an internet search of the jurisdiction it provides designated services to in order to remain aware of changes in the perceived ML/TF risk of that jurisdiction;

- (iii) Shinyuan will train its staff to understand the complexities of the designated services in Section 9.3; and
 - (iv) Shinyuan will ensure that its strict KYC and verification procedures in relation to all customers being provided designated services are applied consistently within the company.
- 9.5. Prior to a new designated service being introduced to the market by Shinyuan, the AML/CTF Compliance Officer will assess it to determine whether it involves a new or increased ML/TF risk.
- 9.6. Prior to the adoption of a new method of delivering a designated service, the AML/CTF Compliance Officer will assess it to determine whether it involves a new or increased ML/TF risk.
- 9.7. Prior to the adoption of a new technology used for the provision of a designated service, the AML/CTF Compliance Officer will assess it to determine whether it involves a new or increased ML/TF risk.
- 9.8. With respect to any changes in the nature of the business relationship, control structure of beneficial ownership of Shinyuan's customers, the AML/CTF Compliance Officer will identify, mitigate and manage any new or increased ML/TF risk.
- 9.9. In making this assessment, the Officer will:
 - (a) Take into account the nature, size and complexity of Shinyuan's business; and how this will change with the new introduction or adoption;
 - (b) Deem there to be a significant change in ML/TF risk where there is a change in one of either the customer type, type of designated service provided, delivery of designated service or foreign jurisdiction or customer business relationship;
 - (c) Assess the compatibility of Shinyuan's AML/CTF Program with the new or increased ML/TF risk;
 - (d) Produce a report of the Officer's:
 - (i) findings in relation to new or increased ML/TF risks; and
 - (ii) recommendations of appropriate changes to the Program;
 - (e) Present the report to Shinyuan's Board, to effect implementation of the recommendations.
 - (f) A copy of the Officer's report must be kept on record.
 - (g) Where it is determined that a new or increased ML/TF risk is involved, the AML/CTF Compliance Officer will recommend amendment of Shinyuan's AML/CTF Program and its practices, to reflect the change.
 - (h) Any risk-based procedure included in Part B will only be appropriate if it takes into account the nature, size and complexity of Shinyuan's business, as well as the type of ML/TF risks it might face. The AML/CTF

Compliance Officer must abide by this principle when assessing a new or increased ML/TF risk. The Officer must have regard to the ML/TF risks relevant to Shinyuan's provision of designated services.

10. APPLICATION OF PART A

- 10.1. Part A of this Program applies to Shinyuan 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.
- 10.2. The procedures in Part A apply on and from the date the Board of Directors assents to this Program.

11. THE AML/CTF COMPLIANCE OFFICER

- 11.1. Shinyuan's AML/CTF Compliance Officer is:
 - (a) Mr. Pei Wang, who is appointed by Shinyuan as its Nominated Contact Officer for the purposes of the AML/CTF Rules.
 - (b) Ms. Yelous Song, who is also appointed by Shinyuan as its Nominated Contact Officer for the purposes of AML/CTF Rules.
- 11.2. The AML/CTF Compliance Officer will at all times:
 - (a) Be a part of the management of Shinyuan;
 - (b) Report directly to the Board of Directors of Shinyuan; and
 - (c) Possess sufficient skills and experience to carry out the role of the AML/CTF Compliance Officer; and
 - (d) Have all authority and resources necessary to carry out their responsibilities effectively, which includes but is not limited to:
 - (i) Access to all relevant areas of business;
 - (ii) Access to all relevant employees;
 - (iii) Power to deal with problems relating to AML/CTF obligations.
- 11.3. The AML/CTF Compliance Officer may occupy multiple roles within the organisation.
- 11.4. The AML/CTF Compliance Officer is responsible for the maintenance of the registration information. This includes reporting any material effects, and updating the business profile form and details, within 14 days of any change in circumstances relating to Shinyuan's registration.
- 11.5. The AML/CTF Compliance Officer is responsible for implementing and overseeing Shinyuan's obligations under the AML/CTF Act and Rules in accordance with Shinyuan's compliance procedures, including the ongoing maintenance of registration information which includes updating the business profile form and updating details in the reporting entity roll within 14 days when required.
- 11.6. The AML/CTF Compliance Officer is authorised to delegate any of his/her

responsibilities under this Program, the AML/CTF Act or Rules to another Shinyuan employee, agent or responsible third party provided it is reasonable to do so. The AML/CTF Compliance Officer's responsibilities may be undertaken in conjunction with an external compliance consultant.

- 11.7. Although the AML/CTF Compliance Officer is authorised to delegate any of his/her responsibilities under this Program, the Compliance Officer still retains ultimate responsibility for implementation and ongoing assessment of this Program.

12. EMPLOYEE DUE DILIGENCE PROGRAM

- 12.1. Shinyuan recognises that various roles within the organisation are potentially able to be abused by those attempting to commit ML/TF offences. It is recognised that different roles have different inherent ML/TF risks and the following sections outline the procedures that ensure that such risks are taken into account.

12.2. 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 ML or TF offence.
- (c) In respect to all prospective employees who, if employed (to fill a newly created role that is able to facilitate a ML/TF transaction, or a previously-existing role that is now able to facilitate a ML/TF transaction), may be in a position to facilitate the commission of a ML or TF 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 (e) below);
 - (vi) carry out a check of whether the person has been subject to disciplinary action by a regulator or legal action or has any matters to be considered before a court of law;

- (vii) carry out a bankruptcy/credit check; and
- (viii) carry out a check of whether the person has lived in high-risk countries (for example, countries that are subject to sanctions by Australia).
- (d) Steps (i), (ii) and (iii) in Section 13.2(c) of this Program will be carried out for all prospective employees regardless of their position at Shinyuan.
- (e) Steps (iv)-(viii) in Section 13.2(c) of this Program will be carried out at the discretion of the AML/CTF Compliance Officer having regard to the ML/TF risk associated with the position of the prospective employee.
- (f) The procedures in Section 13.2 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 ML/TF risk associated with the position of the prospective employee.
- (g) If a prospective employee fails, without reasonable excuse, to comply with these procedures, then Shinyuan may decide not to offer that person employment.
- (h) Employment contracts issued will include a clause stating that employment within Shinyuan is conditional on passing the checks outlined in Shinyuan's AML/CTF 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 Shinyuan may withdraw the offer.

12.3. 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 ML or TF 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 ML or TF 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 Shinyuan's Compliance Officer. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

12.4. Copies of employee checks undertaken in accordance with Sections 13.2 and 13.3 of this Program will be kept in accordance with the Shinyuan's Document Retention Policy.

12.5. Managing Non-Compliance

(a) Shinyuan 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.

13. RISK AWARENESS TRAINING PROGRAM

13.1. The Risk Awareness Training Program ("**RATP**") is designed to ensure each employee of Shinyuan receives appropriate ongoing training on the ML/TF risk that Shinyuan may face.

13.2. Part of Shinyuan's AML/CTF training comprises all relevant staff completing Shinyuan's formulated in-house education program.

13.3. The RATP is designed to enable Shinyuan's employees to understand:

(a) Shinyuan's obligations under the AML/CTF Act and Rules;

(b) the consequences of non-compliance with the AML/CTF Act and Rules;

(c) the type of ML/TF risk that Shinyuan might face and the potential consequences of such risk;

(d) in particular, the ML/TF risk posed by the remittance services Shinyuan provides and the jurisdictions with which it deals; and

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

13.4. Ongoing Compliance Training

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

(b) These updates are made available to all relevant employees of Shinyuan.

13.5. Employee AML/CTF Seminars

- (a) The AML/CTF Compliance Officer will organise AML/CTF seminars covering the AML/CTF issues faced by Shinyuan. These seminars will cover all issues in Section 14.3 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 ML/TF 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 Shinyuan'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 Managing 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.

13.6. Document Retention Policy

- (a) The AML/CTF Compliance Officer will require each:
 - (i) new employee to read a copy of Shinyuan's Document Retention Policy within a reasonable time of commencing their employment; and
 - (ii) Employee to read a copy of Shinyuan'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 Shinyuan's Document Retention Policy will be reported to the Managing Director. Appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Officer.

14. OUTSOURCING

14.1. Where Shinyuan outsources any of its AML/CTF obligations, 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 policies and procedures similar to those outlined in this AML/CTF Program;
- (c) assess the ML/TF 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 ML/TF risk faced by Shinyuan;
- (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 ML/TF risk faced by Shinyuan;
- (f) ensure that all parties to whom the activities and services are outsourced understand:
 - (i) Shinyuan's obligations under the AML/CTF Act and Rules;
 - (ii) the consequences of non-compliance with the AML/CTF Act and Rules;
 - (iii) the type of ML/TF risk Shinyuan 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.

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

- 15.1. Shinyuan does not provide designated services through permanent establishments in foreign countries.
- 15.2. If at any time Shinyuan 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.

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

- 16.1. 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; and
- 16.2. A copy of these records will be retained for at least seven (7) years

after Shinyuan has ceased to provide designated services to the relevant customer.

- 16.3. A copy of any other record made by Shinyuan 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.

17. SUSPICIOUS MATTER REPORTING

- 17.1. If an employee or representative of Shinyuan 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 ML or TF 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 ML or TF offence,
- (c) the employee must **immediately** notify the AML/CTF Compliance Officer.

- 17.2. 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.

- 17.3. If the AML/CTF Compliance Officer receives a notification from an employee or representative under Section 18.1 of this Program, the AML/CTF Compliance Officer must immediately assess the information provided by the employee which led the employee to form a suspicion and determine whether a suspicious matter report should be lodged. Shinyuan is only taken to have formed the relevant suspicion when the AML/CTF Compliance Officer forms the relevant suspicion. Shinyuan is not taken to have formed the relevant suspicion at the time the employee notifies the AML/CTF Compliance Officer.

- 17.4. If the AML/CTF Compliance Officer determines there are reasonable grounds for suspicion and that a suspicious matter report must be lodged in relation to a customer, Shinyuan will:

- (a) apply the enhanced customer due diligence program outlined in this Program; and
 - (b) report the suspicion through its 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 TF; or
 - (ii) in all other cases, within three (3) business days after the time when the AML/CTF Compliance Officer forms the relevant suspicion.
- 17.5. If the AML/CTF Compliance Officer is notified of a suspicion relating to the identity of the customer, the AML/CTF Compliance Officer is not taken to have formed the relevant suspicion requiring lodgement of a Suspicious Matter Report. The AML/CTF Compliance Officer must, within three (3) days commencing after the day on which the AML/CTF Compliance Officer was notified of the suspicion, do one (1) of the following for the purpose of enabling the RE 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.
- 17.6. If:
- (a) after collecting additional KYC Information from a customer in accordance with Section 18.5 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 will have formed the relevant suspicion and must make a suspicious matter report to AUSTRAC.
- 17.7. 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.
- 17.8. A report to AUSTRAC’s CEO of any of the matters set out at Section 18.1 of this Program must be in the approved form and sent in accordance with the requirements of the AML/CTF Act and Rules.
- 17.9. A representative of Shinyuan must not disclose to someone other than

AUSTRAC's CEO or an AUSTRAC staff member:

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

17.10. 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.

18. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

18.1. Where Shinyuan 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 Shinyuan in the identification, management and mitigation of ML/TF risk, the AML/CTF Compliance Officer may request the customer to provide Shinyuan with any such information. The request must be provided in writing and notify the customer that if the request is not complied with, then Shinyuan 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.

18.2. 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, Shinyuan 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.

18.3. 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 17 of this Program).

19. ONGOING CUSTOMER DUE DILIGENCE – OVERVIEW

- 19.1. Shinyuan will monitor its customers with a view to identifying, mitigating and managing the risk that the provision of a designated service by a RE at or through a permanent establishment in Australia may involve or facilitate ML or TF.
- 19.2. The ongoing customer due diligence procedure, which includes the transaction monitoring program, the enhanced due diligence program and collection and verification of KYC information, must be applied to customers.
- 19.3. Shinyuan must undertake reasonable measures to keep, update and review the documents, data or information collected in respect of customer and beneficial owner identification and verification.
- 19.4. Shinyuan will monitor its customers by implementing systems to:
 - (a) as a minimum, collect information to determine the purpose of the remittance and the source of funds and wealth for every customer;
 - (b) collect further KYC Information for ongoing customer due diligence processes;
 - (c) update and verify KYC Information for ongoing customer due diligence purposes;
 - (d) monitor the transactions of customers; and
 - (e) conduct enhanced customer due diligence in respect of high- risk customers and customers about whom a suspicion has been formed.
- 19.5. As part of implementing systems for ongoing customer due diligence purposes, Shinyuan 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.
- 19.6. Please refer to Shinyuan's 'Risk Register' for a generic risk profiling that classifies the client taking into consideration the customer type (including whether the client is a politically exposed person), the types of designated services it provides, the methods by which it delivers designated services; and the foreign jurisdictions with which it deals.

20. ADDITIONAL KYC INFORMATION

- 20.1. In undertaking the risk assessment for new activities and technologies referred to in Section 10 of this Program, additional KYC information will be collected from customers who have a rating of either Medium or High when assessed under section 31.1 either before any designated services are provided to the customer or during the course of the RE's relationship with the customer.
- 20.2. Based on the assessed level of a ML/TF risk involved in the provision of designated services provided by Shinyuan on the date that this Section of this Program was adopted, Shinyuan has determined that no additional KYC Information needs to be collected in relation to low-risk customers. The additional KYC information required to be collected, in respect of medium and high-risk customers is set out in section 32.3
- 20.3. 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.
- 20.4. Shinyuan 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 is likely to be incomplete or unreliable;
 - (b) a representative of a RE becomes aware that KYC Information held in respect of a customer 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 equals or exceeds \$10,000 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.
- 20.5. 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, Shinyuan will carry out the applicable customer identification procedure in accordance with Part B of this Program and collect the relevant additional KYC Information.
- 20.6. Where a change in customer information relates to in the case of:
 - (a) individual customers, the customer's:
 - (i) name;

- (ii) date of birth; or
- (iii) residential address;
- (b) a company:
 - (i) the company's name; or
 - (ii) the company's registration number;

Shinyuan will seek to verify the updated KYC Information using reliable and independent documentation in accordance with Section 51 of this Program.

21. TRANSACTION MONITORING PROGRAM

- 21.1. This Section describes the transaction monitoring program adopted by Shinyuan 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 17 of this Program).
- 21.2. The transaction monitoring program should have regard to complex, unusual, and large transactions which have no apparent economic or visible lawful purpose.
- 21.3. The AML/CTF Compliance Officer must identify ML/TF risk factors relevant to customers of particular services and products provided by the relevant RE, which may involve the provision of a designated service and to representatives of such customers. Such risk factors include, but are not limited to, the:
 - (a) volume of transactions conducted by a customer within a five (5) calendar day period has increased by more than one hundred percent (100%);
 - (b) transaction involves foreign countries, customers or third parties against whom sanctions have been imposed or have been included on either of the lists:
 - (i) maintained by the Department of Foreign Affairs and Trade under the *Charter of United Nations (Terrorism and Dealings with Assets) Regulations 2002* (Cth); or
 - (ii) maintained by the Office of Foreign Assets Control; or
 - (iii) contained in the *Criminal Code Regulations 2002* (Cth); or
 - (c) transaction involves a customer or third party who is a PEP (refer to Section 53 of this Program).
- 21.4. In addition to the Risk Awareness Training referred to in Section 13 of this Program, the AML/CTF Compliance Officer will ensure that all employees of Shinyuan, who have direct contact with customers or their representatives, receive regular training in the identification of relevant ML/TF risk factors, including those associated with remittance services.

- 21.5. An employee of Shinyuan must immediately inform the AML/CTF Compliance Officer when any ML/TF risk factor(s) are identified in relation to a customer or a customer's representative.
- 21.6. Where an employee of Shinyuan identifies a customer or third party of a kind specified in Section 21.3(c) or 21.3(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.
- 21.7. If it is determined, as a result of transaction monitoring, that:
- (a) a customer should be placed in a higher risk grouping, Shinyuan will collect additional KYC Information if required as referred to in Section 20 of this Program;
 - (b) KYC Information needs to be updated or verified in respect of a customer, Shinyuan will update or verify the required information in accordance with Section 20 of this Program;
 - (c) a customer is a high-risk customer, Shinyuan will apply the enhanced customer due diligence program in accordance with Section 22 of this Program; or
 - (d) a suspicious matter report needs to be lodged in respect of a customer, Shinyuan will follow the procedure outlined in Section 17 of this Program.

22. ENHANCED CUSTOMER DUE DILIGENCE PROGRAM

- 22.1. This enhanced customer due diligence program will be implemented in the following circumstances:
- (a) the ML/TF risk associated with a particular designated service, customer, delivery method or jurisdiction is high;
 - (b) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act (refer to Section 17 of this Program);
 - (c) a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign politically exposed person;
 - (d) the reporting entity is entering into or proposing to enter into a transaction and a party to the transaction is physically present in, or is a corporation incorporated in, a prescribed foreign country.
- 22.2. The AML/CTF Compliance Officer will undertake measures appropriate to those circumstances, which may include one of the following:
- (a) Seek information from the customer or from third party sources in order to undertake one of the following:
 - (A) Clarify or update KYC information already collected from the

customer;

- (B) Clarify or update beneficial owner information already collected from the customer;
 - (C) Obtain any further KYC information or beneficial owner information, including, where appropriate, 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;
 - (D) Clarify the nature of the customer's ongoing business with the reporting entity;
- (b) Undertake more detailed analysis of the customer's KYC information and beneficial owner information, including, where appropriate, 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 in accordance with the customer identification program;
 - (d) Verify or re-verify beneficial owner information in accordance with beneficial owner identification requirements in accordance with Section 53 of this Program.
 - (e) Undertake more detailed analysis and monitoring of the customer's transactions – both past and future, including, but not limited to:
 - (i) The purpose, reasons for, or nature of specific transactions; or
 - (ii) The expected nature and level of transaction behaviour, including future transactions;
 - (f) Seek senior management approval for:
 - (i) Continuing a business relationship with a customer; and
 - (ii) Whether a designated service should continue to be provided to the customer;
 - (g) Consider whether a transaction or particular transactions should be processed.

22.3. If the circumstances in section 22.1(c) arise, then in addition to any other measures from section 22.2, the AML/CTF Compliance Manager must undertake the measures in section 22.2(b) and section 22.2(f)

23. REVIEW OF THE AML/CTF PROGRAM

- 23.1. The AML/CTF Compliance Officer must regularly assess Shinyuan's ML/TF 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 ML/TF risk relating to designated services provided by Shinyuan;
 - (b) prior to Shinyuan introducing a new designated service to the market;
 - (c) prior to Shinyuan adopting a new method of delivering a designated service;
 - (d) prior to Shinyuan adopting a new technology or developing technology used for the provision of an existing or new designated service; and
- 23.2. The review is to be undertaken by either an internal or external party, or both. The reviewer must be a person who was not involved in undertaking any of the functions or measures being reviewed, including the design, implementation or maintenance of Part A of the Program or development of Shinyuan's risk assessment or related internal controls.
- 23.3. Shinyuan must be able to demonstrate the independence of any reviewer.
- 23.4. Internal
- (a) Due to the relatively small number of staff members at Shinyuan , internal reviews will not be carried out unless the AML/CTF Compliance Officer considers it necessary or subject to section 23.4(b) of this Program. However, an internal review must take place at least annually.
 - (b) Internal reviews may be carried out where required by Shinyuan's Board of Directors.
 - (c) The internal party conducting the review should:
 - (i) have unlimited access to the records, personnel and property of Shinyuan within the context of Shinyuan's obligations under the *Privacy Act* 1988;
 - (ii) be impartial and objective in performing their duties and should not be inappropriately influenced by management of Shinyuan ; and
 - (iii) not be subject to the requirements of the AML/CTF program.
 - (d) The AML/CTF Compliance Officer will report the results of the internal review to the Board of Shinyuan.
 - (e) The internal review will:
 - (i) assess the effectiveness of Part A of this Program having regard

- to the ML/TF risk of Shinyuan;
- (ii) assess whether Part A of this Program complies with the AML/CTF Rules;
 - (iii) assess whether Part A of this Program has been effectively implemented;
 - (iv) assess whether Shinyuan has complied with Part A of this Program;
 - (v) assess the risk management resources available to Shinyuan including, but not limited to:
 - (A) funding; and
 - (B) staff allocation;
 - (vi) identify any future needs relevant to the nature, size and complexity of Shinyuan; and
 - (vii) assess the ongoing risk management procedures and controls in order to identify any failures.
- (f) When assessing ongoing risk management procedures and controls in order to identify any failures, the internal party conducting the review may have regard to:
- (i) any market information relevant to the global AML/CTF environment which may have an impact on the ML/TF risk faced by Shinyuan;
 - (ii) failure to include all mandatory legislative components in Shinyuan's AML/CTF Program;
 - (iii) failure to gain approval from Shinyuan's Managing Director of this Program;
 - (iv) insufficient or inappropriate employee due diligence;
 - (v) frequency and level of risk awareness training not aligned with potential exposure to AML/CTF risk(s), including AML/CTF risks associated with remittance services;
 - (vi) changes in business functions which are not reflected in this Program (for example, the introduction of a new product or distribution channel);
 - (vii) failure to consider general guidance material or feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);
 - (viii) failure to undertake an independent review (at an appropriate level and frequency) of the content and application of this Program;

- (ix) legislation incorrectly interpreted and applied in relation to a customer identification procedure;
- (x) customer identification and monitoring systems, policies and procedures that fail to:
 - (A) prompt, if appropriate, for further identification and/or verification to be carried out when the AML/CTF risk posed by a customer increases;
 - (B) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;
 - (C) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
 - (D) take appropriate action where the identification document provided is neither an original nor a certified copy;
 - (E) recognise foreign identification issued by a high-risk jurisdiction;
 - (F) record details of identification documents, for example, the date of issue;
 - (G) consult appropriate resources in order to identify high-risk customers;
 - (H) identify when an expired or old identification document (for example, a driver's licence) has been used;
 - (I) collect any other name(s) by which the customer is known;
 - (J) be subject to regular review;
- (xi) 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;
- (xii) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
 - (A) customer identification policies, procedures and systems; and
 - (B) identifying potential AML/CTF risks;
- (xiii) assess the acceptance of documentation that may not be readily verifiable.
- (g) If the AML/CTF Compliance Officer determines it is appropriate, the internal review may also:
 - (i) assess whether the risk-based procedures and processes

adopted in this Program have changed such that alterations need to be made to the AML/CTF Program;

- (ii) assess whether Part B of this Program is sufficient to cover the ML/TF risks posed by existing and potential customers of Shinyuan; and
- (iii) 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.

23.5. External

- (a) The AML/CTF Compliance Officer will arrange for this Program to be reviewed by an external party at least once every three years or more frequently, subject to changes to the risk profile of Shinyuan, legislative developments and market information regarding ML/TF risk. Additional external reviews may be carried out where the AML/CTF Compliance Officer considers it necessary.
- (b) Prior to engagement of the external party, the AML/CTF Compliance Officer will document the reasons for determining their independence.
- (c) The AML/CTF Compliance Officer will report the results of the external review to the Board of Directors for Shinyuan.
- (d) The external review will:
 - (i) assess the effectiveness of Part A of this Program having regard to the ML/TF risk of Shinyuan;
 - (ii) assess whether Part A of this Program complies with the AML/CTF Rules;
 - (iii) assess whether Part A of this Program has been effectively implemented;
 - (iv) assess whether Shinyuan has complied with Part A of this Program;
- (e) The AML/CTF Compliance Officer may also require the external party conducting the review to:
 - (i) assess the ongoing risk management procedures and controls to identify any failures including, but not limited to:
 - (A) failure to include all mandatory legislative components in Shinyuan's AML/CTF Program;
 - (B) failure to gain approval from Shinyuan's Board of Directors of this Program;
 - (C) insufficient or inappropriate employee due diligence;
 - (D) frequency and level of risk awareness training not aligned

with potential exposure to AML/CTF risk(s), including AML/CTF risks associated with remittance services;

- (E) changes in business functions which are not reflected in this Program (for example, the introduction of a new product or distribution channel);
- (F) failure to consider general guidance material or feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);
- (G) failure to undertake independent review (at an appropriate level and frequency) of the content and application of this Program;
- (H) legislation incorrectly interpreted and applied in relation to customer identification procedures;
- (I) 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;
- (J) 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;

- (K) 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;
- (ii) assess the acceptance of documentation which may not be readily verifiable;
- (iii) assess the risk management resources available to Shinyuan including, but not limited to:
 - (A) funding; and
 - (B) staff allocation; and
- (iv) identify any future needs relevant to the nature, size and complexity of Shinyuan.
- (f) If the external reviewer determines it is appropriate, the external review may also:
 - (i) assess whether the risk-based procedures and processes adopted in this Program have changed such that alterations need to be made to this Policy;
 - (ii) assess whether Part B of this Program is sufficient to cover the ML/TF risks posed by existing and potential customers of Shinyuan; and
 - (iii) assess whether any additional changes need to be made to this Program as a result of changes to the AML/CTF regulations and legislation and the AML/CTF environment generally.

24. AUSTRAC FEEDBACK

24.1. Where AUSTRAC provides Shinyuan with general guidance material or feedback specific to Shinyuan regarding performance on the management of ML/TF 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 25 of this Program.

25. OVERSIGHT BY THE MANAGING DIRECTOR / UPDATING THE PROGRAM

25.1. This Program is approved by the Board of Directors of Shinyuan. The Board of Directors is informed by the Managing Director of any changes made to this Program and will approve later versions of the program and this will be recorded in the minutes to the meeting. The Managing Director will sign

the Version Control Table.

- 25.2. The AML/CTF Compliance Officer will report to the Managing Director of Shinyuan on a regular basis in relation to:
- (a) significant changes to the ML/TF risks affecting Shinyuan's reporting entities;
 - (b) compliance with this Program, the AML/CTF Act and Rules by Shinyuan;
 - (c) the results of and any report produced for any internal or external review of this Program;
 - (d) any AUSTRAC guidance material or feedback; and
 - (e) changes to relevant legislation.
- 25.3. 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 25.2 of this Program. Subject to Section 25.4 of this Program, such amendments should be considered and approved by the Board of Directors of Shinyuan before they become effective.
- 25.4. 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 Board of Directors' approval can occur. In these circumstances, the AML/CTF Compliance Officer should seek the Managing Director's approval, of a change, as soon as reasonably practical after it is made. The Managing Director's approval must nevertheless be attained as soon as reasonably practical following the change.

26. REPORTS TO BE LODGED WITH AUSTRAC

- 26.1. Suspicious Matter Reporting:
- (a) Shinyuan has implemented Suspicious Matters Reporting ("SMR") procedures to meet its SMR reporting obligations. Details are set out in section 17.
- 26.2. International Funds Transfer Instructions Reporting:
- (a) An International Funds Transfer Instruction ("IFTI") is an instruction sent between banks (or through a designated remittance arrangement) to transfer money.
 - (b) Shinyuan is responsible for reporting obligations in relation to IFTIs that arise from all transactions Shinyuan facilitates under its designated remittance arrangement.
 - (c) Shinyuan has implemented IFTI Reporting procedures to meet its IFTI reporting obligations if and when they arise (refer Annexure A).

- (d) The AML/CTF Compliance Officer will be trained to prepare, lodge and retain records for IFTI reporting.
- (e) Under section 45(2) of the AML/CTF Act, Shinyuan must within 10 business days after the day on which the international funds transfer instruction was sent or received, provide a report to AUSTRAC.

26.3. AML/CTF Compliance Report

- (a) Under section 47(2) of the AML/CTF Act, Shinyuan is required to periodically provide an AML/CTF compliance report to AUSTRAC. This report sets out a reporting entity's compliance with the AML/CTF Act and Regulations. The report contributes to AUSTRAC's monitoring of ongoing industry compliance with the AML/CTF Act.
- (b) The AML/CTF Officer is required to diarise the lodgement date for each reporting period. The reporting period relates to January to December each year, and the report must be lodged by the end of March the following year.
- (c) In preparing the report, the AML/CTF Officer must carefully review all questionnaire questions and accurately complete the report. The statements in the report must accurately reflect the policies and procedures set out in the AML/CTF Program. During the course of completing the report, if weaknesses in Shinyuan's policies and procedures are identified, the AML/CTF Officer must submit a report to the Board of Directors, together with a rectification plan.
- (d) The rectification plan must be implemented as soon as practicable and follow up review must be undertaken to ensure that the plan has been implemented effectively.

26.4. Changes to the Reporting Entity's Enrolment Details

- (a) Under section 51F of the AML/CTF Act, Shinyuan is required to advise the AUSTRAC CEO of any change in Shinyuan's enrolment details. The AML/CTF Compliance Officer is responsible for advising the AUSTRAC CEO of matters as outlined in Chapter 64 of the AML/CTF Rules.
- (b) The Compliance Officer is also responsible for reporting material changes to Shinyuan's registration information to AUSTRAC.
- (c) Shinyuan must advise the AUSTRAC CEO within 14 days of the change arising.

PART B – CUSTOMER IDENTIFICATION

27. INTRODUCTION

- 27.1. **Part B** of this Program sets out the customer identification procedures for Shinyuan's customers. If it includes customer types that Shinyuan does not currently provide services, please ignore those sections.
- 27.2. 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 ML/TF risk relevant to the provision of Shinyuan's designated services.
- 27.3. Shinyuan will consider the following factors when identifying its exposure to ML/TF and developing its customer identification procedures, the:
- (a) customer types; including:
 - (i) beneficial owners of customers; and
 - (ii) any politically exposed persons;
 - (b) customer's sources of funds and wealth;
 - (c) nature and purpose of the business relationship with its customers, including, as appropriate the collection of information relevant to that consideration;
 - (d) control structure of its non-individual customers;
 - (e) types of designated services provided;
 - (f) methods by which those services are delivered; and
 - (g) country in which those services are delivered.

28. APPLICATION OF PART B

- 28.1. Part B of this Program applies to Shinyuan, including any functions carried out by a responsible third party.

29. KYC – CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES

- 29.1. The customer identification and verification procedures must be carried out by Shinyuan or a responsible third party:
- (a) prior to commencing to provide a designated service to a customer (other than an existing customer), unless Shinyuan has already carried out the applicable customer identification procedure in

respect of the customer; and

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

30. KNOW YOUR CUSTOMER – CONSIDERATIONS

- 30.1. Once information relating to a customer has been collected and verified, Shinyuan will re-assess the ML/TF risk posed by the customer.
- 30.2. In re-assessing the AML/CTF Customer Type Risk for Shinyuan, it may consider, where appropriate and among other factors, whether:
 - (a) the customer is involved in a complex business ownership structure with no legitimate commercial rationale;
 - (b) 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;
 - (c) the customer is in a position which may expose Shinyuan to the possibility of corruption;
 - (d) the customer is based in, or conducting business through or in, a high-risk jurisdiction;
 - (e) the customer is engaged in business which involves significant amounts of cash;
 - (f) there is no clear commercial rationale for the customer seeking a designated service;
 - (g) the customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting transactions;
 - (h) the customer is a PEP;
 - (i) the customer uses multiple bank accounts for no apparent commercial or other reason;
 - (j) an undue level of secrecy is requested regarding a designated service;
 - (k) the source of funds is difficult to verify;
 - (l) the beneficial owners of a non-individual customer are difficult to identify and/or verify;
 - (m) the beneficial owners of the non-individual customer are a resident in a high-risk jurisdiction;

- (n) there is a one-off transaction in comparison with an ongoing business relationship or series of transactions;
- (o) a designated service can be used for ML or TF (and the extent to which it can be used);
- (p) the customer makes or accepts payments (for example, electronic transfers) to or from accounts which have not been identified by the RE;
- (q) the customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts;
- (r) the customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer);
- (s) the customer when migrating from one designated service to another carries a different type and level of AML/CTF risk;
- (t) the customer has income which is not employment-based or from a regular known source;
- (u) the customer is new, rather than having a long-term and active business relationship with the RE;
- (v) the customer's business is registered in a foreign jurisdiction with no local operations or domicile;
- (w) the customer's business is an unregistered charity, foundation or cultural association;
- (x) the customer is represented by another person, such as under a power of attorney.

31. INDIVIDUALS: CUSTOMER IDENTIFICATION PROCEDURES

31.1. Where a new customer is an individual (other than an individual who notifies the RE that he or she is a customer of Shinyuan in his or her capacity as a sole trader), Shinyuan must collect, at a minimum, the customer's:

- (a) full name;
- (b) date of birth; and
- (c) residential address.

31.2. Where a new customer notifies Shinyuan that he or she is a customer in his or her capacity as a sole trader, Shinyuan 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.

31.3. Where the ML/TF risk posed by the provision of a designated service to a particular individual is assessed as medium or high under Section 30.1 of this Program, the AML/CTF Compliance Officer may require Shinyuan'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 (change of name certificate);
- (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 (financial statement);
- (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 the RE; and
- (g) details of the customer's employment (e.g. name of employer, length of employment, type of institution).

31.4. The information collection requirements in this section are not intended to conflict with any other obligation Shinyuan has under other legislation including the *Privacy Act* 1998. Any conflicts, which arise, should be immediately notified to the AML/CTF Compliance Officer.

32. INDIVIDUALS: VERIFICATION – PRINCIPLES

32.1. At a minimum, the following KYC Information about a customer in section 31 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.

32.2. Where it has been determined that the ML/TF risk posed by the provision of a designated service to an individual is medium or high under the assessment carried out under Section 30.1 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.

- 32.3. Information which is required to be verified as indicated in section 32.2, 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.

33. INDIVIDUALS: VERIFICATION – PROCEDURES

- 33.1. The following verification procedures need to be followed for individuals:
- (a) PEP identification and verification (section 53 of this Program);
 - (b) Foreign high-risk jurisdiction verification (section 51 of this Program); and
 - (c) A document identification procedure (a 'standard customer identification procedure' outlined in sections 33.2 and 33.3 of this Program, should be conducted in all cases where possible).
- 33.2. **Standard domestic documentation identification procedure:** The information in section 33.2, of this Program, can be verified from either an original or certified copy of a current:
- (a) Australian driver's licence containing a photograph of the person;
 - (b) Australian passport (it is also permissible for a passport to be issued by the Commonwealth to have expired within the preceding 2 years); or
 - (c) Card issued under a State or Territory law, for the purpose of proving a person's age, containing a photograph of the person in whose name the card is issued.
- 33.3. **Standard foreign documentation identification procedure:** The information in section 33.2, of this Program, can be verified from either an original or certified copy of a current foreign government issued passport or similar travel document. In addition to a photograph, this document must contain either a signature or any unique identifier in whose name the document is issued. Where any document relied on as part of this procedure is in a language that is not English, it must be accompanied by an English translation prepared by an accredited translator.
- 33.4. **Non-standard customer identification procedures:** The procedures in sections 33.5 and 33.6, of this Program, should only be conducted where:
- (a) a 'standard customer identification procedure' in section 33.2 and 33.3 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.

33.5. **Acceptable ‘non-standard domestic documentation identification procedure’:** An acceptable ‘non-standard domestic documentation identification procedure’ would be based on:

- (a) an original or certified copy of:
 - (i) Australian Birth Certificate;
 - (ii) Australian Citizenship Certificate; or
 - (iii) both:
 - (A) A concession card, as defined in the *Social Security Act 1991*, or an equivalent term which expresses the same concept to concession holders; and
 - (B) an original notice issued to an individual, of a kind listed below, that contains the name of the individual and his or her residential address:
 - (I) issued by the Commonwealth or a State or Territory within the preceding twelve (12) months that records the provision of financial benefits; or
 - (II) issued by the Australian Taxation Office within the preceding twelve (12) months; or
 - (III) issued by a local government body or utilities provider within the preceding three (3) months that records the provision of services to that address or to that person.

33.6. **Acceptable ‘non-standard foreign documentation identification procedure’:** In general, Shinyuan should be cautious about arranging for the provision of a product or service for a customer who presents foreign based identification which is not a passport. However, in the event the customer has not presented a passport, an example of an acceptable ‘non-standard foreign documentation identification procedure’ would be based on either an original or certified copy of a current:

- (a) National Identity Card issued by a foreign government containing a photograph and either a signature or other unique identifier of the person in whose name the card is issued;
- (b) Foreign driver’s licence which contains a photograph of the person in whose name it was issued; and
- (c) Where any document relied on as part of the procedure is in a language that is not English, it must be accompanied by an English translation prepared by an accredited translator.

33.7. When determining whether to accept non-standard foreign documentation,

the AML/CTF Compliance Officer should have regard to the ML/TF risk posed by the provision of a designated service to a customer from that particular foreign country.

33.8. For the purposes of verification of an individual, Shinyuan must have regard to the ML/TF 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 56 of this Program.

33.9. **Alternative data:** There may be limited and exceptional circumstances where a customer has a legitimate reason for being unable to provide satisfactory evidence of their identity. Such circumstances include, but is not limited to:

- (a) The individual's birth was not registered
- (b) People who are homeless
- (c) Undocumented arrivals in Australia
- (d) People affected by natural disasters
- (e) People with limited access to identify documents
- (f) Young people or those under 18 who have not established a 'social footprint'.

33.10. In these circumstances, the AML/CTF Compliance Officer may:

- (a) Utilise alternative identity proofing processes, in accordance with Shinyuan's risk-based systems and controls. This may include, but is not limited to, acceptance of multiple types of secondary identification documents where normally a primary identification document would be required.
- (b) If Section 33.10(a) is unsuccessful, accept a self-attestation from the customer certifying that the information provided in relation to their identity is true and correct
 - (i) An entity must not rely on self-attestation if they know or have reason to believe that it is incorrect or misleading.
 - (ii) A reporting entity must apply appropriate levels of ongoing customer due diligence in order to identify, mitigate and manage any ML/TF risk associated with customer identities established using self-attestation.

33.11. The AML/CTF Compliance Officer will consider the risk-rating of the customer in determining whether to apply any alternative identity proofing procedure.

- (a) A person with a risk-rating of medium or high will not be permitted to

utilise this alternative method.

34. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES

34.1. Where a new customer is a company, either domestic or foreign, it is necessary for Shinyuan's employee who is responsible for that customer to be reasonably satisfied that:

- (a) the company exists; and
- (b) in respect of certain companies, the name and address of any beneficial owner of the company has been provided (see Section 35 of this Program).

34.2. **Information Collection:** The following KYC Information must be collected by Shinyuan's employee who is responsible 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/ABN 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.

34.3. Where the ML/TF risk posed by the provision of a designated service to a particular company is assessed as medium or high under Section 30.1 of this Program, the AML/CTF Compliance Officer may require Shinyuan's employee responsible for the customer 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 Managing Director or CEO (if any);
- (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.

34.4. The AML/CTF Compliance Officer may also determine, where the ML/TF risk posed by the company is medium or high, that the individuals referred to in Sections 34.3(f) and 34.3(g), of this Program, must be screened against the lists mentioned in Section 53.1 of this Program.

34.5. The verification procedures in Section 36, of this Program, must also be followed, having regard to the ML/TF risk relevant to the provision of the designated service.

35. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES – BENEFICIAL OWNERS

35.1. Where a new customer is a company, either domestic or foreign, that is a proprietary or private company (other than a proprietary company that is licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company, or a foreign-listed public company or a majority-owned subsidiary of a foreign-listed public company that is already subject to beneficial ownership disclosure requirements), it is necessary for Shinyuan's employee responsible for the customer to:

- (a) collect the information referred to in Section 34.2 of this Program; and
- (b) collect and verify the full name and date of birth or full residential address of each individual that is a 'Beneficial Owner'.

35.2. Shinyuan must take reasonable measures to verify the information it collects about the beneficial owner. Reasonable measures means that the measures

it takes to verify the information must be appropriate given the assessed level of ML/TF risk.

36. COMPANIES: VERIFICATION – PROCEDURES

36.1. The following verification procedures need to be followed for companies:

- (a) PEP verification (refer to Section 53 of this Program); and
- (b) Foreign high-risk jurisdiction verification (refer to Section 51 of this Program); and
- (c) A document identification procedure (refer to Section 36.2 of this Program).

36.2. At a minimum, the following KYC Information about a customer in Section 34 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) 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 or ABN issued to the company;
 - (v) whether the company is registered by ASIC as a proprietary or public company; and
 - (vi) 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;
 - (iv) the ARBN issued to the company;
 - (v) the country in which the company was formed, incorporated or registered;
 - (vi) 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
 - (vii) 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 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;
 - (D) if the company is registered as a private company by the relevant foreign registration body – the name of each director of the company; and
 - (E) 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.

36.3. 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.

36.4. Where it has been determined under an assessment conducted under Section 30.1, of this Program, that the ML/TF 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.

36.5. For information that is required to be verified as indicated in Section 36.2 of this Program and, the following can be used:

- (a) reliable and independent documentation (refer to Section 38 of this Program);
- (b) reliable and independent electronic data (refer to Section 39 of this Program); or

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

37. COMPANIES: SIMPLIFIED VERIFICATION PROCEDURES

37.1. The criteria in Section 36, of this Program, does not have to be satisfied where Shinyuan confirms that the company is:

- (a) a domestic listed public company;
- (b) a majority owned subsidiary of a domestic listed public company; or
- (c) licenced 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:

- (a) a search of the relevant domestic stock exchange;
- (b) a public document issued by the relevant company;
- (c) a search of the relevant ASIC database; or
- (d) a search of the licence or other records of the relevant regulator.

38. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

38.1. 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 certified by an appropriate officer of the customer that verifies information about the beneficial ownership of a company (subject to Sections 39.2-39.4 and Chapter 30 of the AML/CTF Rules).

38.2. Disclosure Certificates can only be relied upon if:

- (a) Shinyuan 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) Shinyuan has applied the relevant procedures and requirements in this Program, but has been unable to obtain or verify the information and
- (d) The information is one or more of the items of information specified in Chapter 30 of the AML/CTF Rules.

- 38.3. Disclosure Certificates cannot be relied on if:
- (a) Shinyuan knows or has reason to believe that information contained in the certificate is incorrect or unreliable.
- 38.4. Shinyuan has the discretion to determine who is an 'appropriate officer of the customer' in accordance with its risk-based systems and controls.

39. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT ELECTRONIC DATA

- 39.1. When verifying KYC Information collected from a customer by means of reliable and independent electronic data, the procedures below need to be followed.
- 39.2. 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 41.1 of this Program:
- (a) ASIC (www.asic.gov.au);
 - (b) ASX (www.asx.com.au); and
 - (c) APRA (www.apra.gov.au).
- 39.3. 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 40.1 of this Program:
- (a) a search of the relevant foreign stock or equivalent exchange (if any) – refer to section 39.4 of this Program; and
 - (b) a search of the records of the relevant regulator.
- 39.4. 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.

39.5. For the purposes of verification of a foreign listed public company, Shinyuan must have regard to the ML/TF 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 56 of this Program.

40. COMPANIES: VERIFICATION – ALTERNATIVE DATA

40.1. Where the data in Section 39, of this Program, cannot be obtained or is not sufficient to verify the required data listed in Sections 34.2 and 35 of this Program, in consultation with the AML/CTF Compliance Officer, Shinyuan'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.

41. COMPANIES: VERIFICATION – INDEPENDENT CONTACT

41.1. To verify KYC Information collected from a customer, Shinyuan'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.

41.2. Any of the electronic data in Sections 39.2 or 39.3, of this Program, can also be used for the purposes of this Section.

42. TRUSTEES: CUSTOMER IDENTIFICATION PRINCIPLES

42.1. Where a new customer acts in the capacity of a trustee of a trust, it is necessary for Shinyuan's employee responsible for that customer to be reasonably satisfied that:

- (a) the trust exists; and
- (b) the name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided (refer to Section 45 of this Program).

43. EXISTENCE OF THE TRUST – CUSTOMER IDENTIFICATION PROCEDURES

43.1. In accordance with section 42.1(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; or
 - (ii) The settlor is deceased; or
 - (iii) The trust is verified using the simplified trustee verification procedure in Section 47 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 under Section 31 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 under Sections 34 to 35 of this Program;
 - (h) if the trustees comprise 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) under the applicable customer identification procedures in Sections 31 to 33 or Sections 34 to 35 of this Program.
- 43.2. Where it is determined under an assessment carried out under Section 30.1, of this Program, that the ML/TF 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 Shinyuan 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 ML, 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.

44. EXISTENCE OF THE TRUST – VERIFICATION – PROCEDURES

- 44.1. The following verification procedures need to be followed for trusts:
- (a) PEP verification (refer to Section 55 of this Program);
 - (b) Foreign high-risk jurisdiction verification (refer to Section 51 of this Program); and
 - (c) a document identification procedure (refer to Section 44.2 of this Program).
- 44.2. At a minimum, the following KYC Information about a customer in Section 43 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 in accordance with the customer identification procedures in Section 31 of this Program;
- (c) if any of the trustees is a company, then in respect of one of those companies – information about the company in accordance with the procedures in Sections 34 to 35 of this Program; and
- (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) in accordance with the applicable procedures in Section 31 to 33 or Sections 34 to 35 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; or
 - (ii) the settlor is deceased; or
 - (iii) the trust is verified using the simplified trustee verification procedure under Section 48 of this Program.

44.3. Where it has been determined under an assessment carried out under Section 30.1, of this Program, that the ML/TF 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.

45. TRUSTEES AND BENEFICIARIES – CUSTOMER IDENTIFICATION PROCEDURES

45.1. In accordance with section 42.1(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 terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.

46. TRUSTEES AND BENEFICIARIES – VERIFICATION – PROCEDURES

- 46.1. The information collected under Section 42-45 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.
- 46.2. For the purposes of sections 46.1(b) and 46.1(c) of this Program, 'reliable and independent documents relating to the trust' includes a disclosure certificate certified by an appropriate officer of the customer that verifies information about a trust where:
- (a) the verification is being conducted as a result of a risk-based assessment in section 27.2(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 46.1 of this Program.
- 46.3. For the purposes of verification of a trustee, Shinyuan must have regard to the ML/TF 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 56 of this Program.

47. TRUSTEES: SIMPLIFIED VERIFICATION – PROCEDURES

- 47.1. The criteria in Sections 44 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 clients; and
 - (ii) does not make small scale offerings to which section 1012E of the *Corporations Act 2001* (Cth) applies;
 - (c) a government superannuation fund established by legislation.
- 47.2. The criteria in Sections 45-46 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 clients; and
- (ii) does not make small scale offerings to which section 1012E of the *Corporations Act 2001* (Cth) applies; or
- (c) a government superannuation fund established by legislation.

48. AGENTS: IDENTIFICATION PROCEDURES

- 48.1. Where an agent requests the provision of a designated service on behalf of a customer, Shinyuan must collect, at a minimum the following:
- (a) the full name of the person who purports to act on behalf of the customer; and
 - (b) evidence of the customer's authorisation of the person to act on its behalf.
- 48.2. Where an agent requests the provision of a designated service on behalf of a customer, Shinyuan will carry out the relevant customer identification procedure outlined in Part B of this Program, in respect of that customer.

49. AGENTS: VERIFICATION PRINCIPLES

- 49.1. Shinyuan will not verify the identity of the agent where the ML/TF risk associated with the provision of a designated service is classified as low by the AML/CTF Compliance Officer. Where it is determined that the ML/TF risk associated with the provision of a designated service to the particular customer is medium or high, Shinyuan will verify the information specified in Section 48.1 of this Program, in accordance with the requirements of Section 33.4 of this Program.
- 49.2. Shinyuan will verify the identity of the customer in accordance with its customer identification procedures set out in Part B of this Program.

50. VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

- 50.1. 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.
- 50.2. 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 ML/TF 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.
- 50.3. 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.
- 50.4. 'Reliable and independent documentation' includes a disclosure certificate

certified by an appropriate officer of the customer that verifies information prescribed in Chapter 30 of the AML/CTF Rules.

51. VERIFICATION – FOREIGN JURISDICTIONS

- 51.1. Where Shinyuan 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.
- 51.2. The assessment should take into account information from legitimate, respected domestic and/or international bodies.
- 51.3. 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 Shinyuan should continue dealing with the customer.

52. IDENTIFICATION AND VERIFICATION – BENEFICIAL OWNERS

- 52.1. Where Shinyuan has the prospect to acquire a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in this Policy.
- 52.2. Except for Australian Government Entities and foreign-listed public companies/majority-owned subsidiaries of foreign-listed public companies already subject to disclosure requirements that ensure transparency of beneficial ownership, beneficial owners must be identified for all customer types.
- 52.3. For each customer type, Shinyuan must collect and verify the following for each Beneficial Owner:
- (a) Full name;
 - (b) Full residential address; or
 - (c) Date of birth.
- 52.4. With respect to individual customers, Shinyuan assumes that the Beneficial Owner and the customer are the same person unless there are reasonable grounds to consider otherwise.
- 52.5. Where a Beneficial Owner cannot be ascertained:

- (a) Shinyuan must identify and take reasonable measures to verify:
 - (i) For a Company (other than a Company verified under the simplified company verification procedure in Section 37 of this Program) or a Partnership:
 - (A) Any individual who is entitled (directly or indirectly), to exercise 25% or more of the voting rights, including a power of veto; or
 - (B) Any individual who is a senior managing official (or equivalent).
 - (ii) For a Trust (other than a Trust verified under the simplified trustee verification procedure in Section 47 of this Program):
 - (A) Any individual who holds the power to appoint or remove trustees.

53. IDENTIFICATION AND VERIFICATION – POLITICALLY EXPOSED PERSON ('PEP')

- 53.1. Where Shinyuan has the prospect to acquire a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in this Policy.
- 53.2. To identify whether a customer or beneficial owner is a PEP;
- (a) All customers or beneficial owners must self-identify themselves as a PEP; and
 - (b) Shinyuan will use a commercial PEP list provider such as World Check or similar.
- 53.3. If it is determined that a customer is a PEP, Shinyuan will:
- (a) obtain approval from senior management before providing a designated service to the customer;
 - (b) collect information regarding the source of wealth and source of funds used by the customer; and
 - (c) apply the ongoing customer due diligence program outlined in Section 19 of this Program.
- 53.4. If it is determined that a customer is a PEP, Shinyuan will assume that the customer is high risk and must:
- (a) obtain approval from senior management before providing a designated service to the customer;
 - (b) collect information regarding the source of wealth and source of funds used by the customer; and
 - (c) apply the ongoing customer due diligence program outlined in Section 19 of this Program.

- 53.5. If it is determined that a beneficial owner is a PEP, Shinyuan will:
- (a) Follow the customer identification and verification procedures applicable to individuals.
- 53.6. Where the individual is a foreign PEP, carry out the applicable steps in Section 22 of this Program.
- 53.7. All customers of Shinyuan must undergo the PEP determination process.
- 53.8. It is the responsibility of all Shinyuan's employees to be aware of the risks associated with PEP, and Shinyuan employees should closely monitor the transactions conducted by PEP customers.
- 53.9. If a Shinyuan employee suspects that a transaction undertaken by a PEP involves funds that are the proceeds of corruption or other criminal activity, it must report any new information or suspicions immediately to the AML/CTF Compliance Manager.

54. NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF COMPLIANCE OFFICER

- 54.1. The AML/CTF Compliance Officer must be notified of all new customers.
- 54.2. 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.

55. TOLERANCE OF DISCREPANCIES AND ERRORS

- 55.1. **Tolerance of discrepancies:** Where, during the KYC Information collection and verification process, a director, officer or employee of Shinyuan 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. The AML/CTF Compliance Officer is to make a determination as to the significance of the discrepancy. This determination is to be made in consideration of the AML/CTF Customer Type Risk as determined under Section 30. Any discrepancy with new customers with a high-risk rating shall be deemed significant. However, this does not prevent the AML/CTF Compliance Officer from determining a discrepancy with a Low or Medium risk customer to be significant if considered appropriate. Where the discrepancy is significant, independent contact should be initiated with the customer to clarify the information. Should the AML/CTF Compliance Officer not be satisfied with the customer's response, Shinyuan must not take on the new customer and cease all services being provided to them.
- 55.2. **Pre-defined tolerance levels for matches and errors:** Shinyuan 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. Should the AML/CTF Compliance Officer not be satisfied with the customer's response, Shinyuan must not take on the new customer and cease all services provided to them until the information is sufficiently corrected.

56. COMPLIANCE OFFICER TO SIGN

- 56.1. Shinyuan's Compliance Officer is required to give final sign-off on this Program before it made effective.

ANNEXURE A

INTERNATIONAL FUNDS TRANSFER INSTRUCTION REPORTING PROCEDURES

1. Introduction

Shinyuan has an obligation to report international funds transfer instructions (“IFTIs”) to AUSTRAC when it accepts or sends an instruction for money or property to be transferred into or out of Australia.

Shinyuan will identify IFTI transactions and prepare, lodge and retain records of IFTI reporting.

2. International Funds Transfer Instructions (“IFTIs”)

Reporting obligations for IFTIs apply to a reporting entity when they accept or send an instruction for money or property to be transferred into or out of Australia.

2.1 What is an IFTI?

An IFTI is an instruction to transfer money or property into or out of Australia, either electronically or through a designated remittance arrangement. These are also commonly referred to as international wire transfers. (Note: All IFTIs need to be reported to AUSTRAC regardless of transfer value.)

The AML/CTF Act sets out the four IFTI types, the first two of which are based on the definition of an electronic funds transfer instruction (EFTI). The second two involve an ‘instruction given by a transferor entity for the transfer of money or property under a designated remittance arrangement’.

The four types of IFTIs are:

- (i) EFTI (outgoing) – sent through an Australian ordering institution to a beneficiary institution in a foreign country;
- (ii) EFTI (incoming) – sent through an ordering institution in a foreign country to a beneficiary institution in Australia;
- (iii) remittance arrangement (outgoing) – sent through a permanent establishment of a person in Australia to a permanent establishment of a person in a foreign country; and
- (iv) remittance arrangement (incoming) – sent through a permanent establishment of a person in a foreign country to a permanent establishment of a person in Australia.

2.2 IFTIs under a designated remittance arrangement

(a) What is money?

Under the AML/CTF Act ‘money’ includes physical currency, money held in an account, money held on deposit, and digital currency.

What is physical currency?

Physical currency means coin and printed money, including foreign currency, that:

- (a) is designated as legal tender; and
- (b) circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue.

What is digital currency?

Digital currency means either (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) digital currency is a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules.

However, digital currency (as defined in the AML/CTF Act) 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 (no Rules to that effect have been made as at the date of publication of these procedures)

(b) What is property?

The AML/CTF Act defines property as ‘any legal or equitable estate or interest in real or personal property including a contingent or prospective one, but does not include money’. Property refers to a possession or possessions owned by a person that can be tangible or intangible.

(c) What is a remittance arrangement?

In essence, a designated remittance arrangement is one where a person who is **not** an authorised deposit taking institution, bank, building society or credit union accepts money or property from another person and transfers the money or property through another person, who is **not** an authorised deposit-taking institution, bank, building society or credit union, to the ultimate recipient. Often the actual movement of funds will take place through the formal banking system. However, the instruction is transmitted outside the formal banking system.

Items 31 and 32 of table 1 in section 6 in the AML/CTF Act set out the designated services for remitters. For the purposes of IFTI reporting, a

designated remittance arrangement includes only those instructions going out of or coming into Australia.

There are many remittance service providers who use informal systems to transfer funds. These informal systems are usually based on cultural or ethnic structures, and in some cases have been operating for many centuries.

Alternative remittance systems are usually based on trust and rarely issue receipts. Funds can be transferred from one location to another in a manner that is convenient and often cheaper than the formal banking system.

The alternative remittance process for an outgoing IFTI involves three steps:

1. A customer places an order with their chosen remitter.
2. The remitter transmits the details of this order (the payment instruction) to their overseas agent.
3. The agent delivers the funds according to the instruction.

The payment instruction can be transmitted in a variety of ways, including an SMS message, email, fax or telephone call.

2.3 IFTIs involving the electronic transfer of funds

(a) What is an EFTI?

An electronic funds transfer instruction (EFTI) is an instruction that is sent between an ordering and beneficiary institution for the purpose of transferring funds. An ordering institution or beneficiary institution must be an authorised deposit-taking institution, bank, building society, credit union or a person specified in the AML/CTF Rules, for the EFTI to take place.

There are four types of EFTIs set out in the AML/CTF Act:

- a multiple-institution person-to-person electronic funds transfer instruction
- a same-institution person-to-person electronic funds transfer instruction
- a multiple-institution same-person electronic funds transfer instruction, and
- a same-institution same-person electronic funds transfer instruction.

(b) When is an EFTI an IFTI?

An EFTI is an IFTI when the instruction is to transfer funds out of Australia to a foreign country or into Australia from a foreign country. EFTIs include instructions for domestic transfers as well as international transfers. It is important to remember that an EFTI can occur only between authorised deposit-taking institutions, banks, building societies, credit unions or persons specified in the AML/CTF Rules.

2.4 Who is responsible for reporting IFTIs to AUSTRAC?

If Shinyuan is the sender of an IFTI transmitted out of Australia, or if Shinyuan receives an IFTI transmitted into Australia, it must report the instruction to AUSTRAC.

Shinyuan's AML /CTF Compliance Officer is responsible for providing the IFTI report to AUSTRAC.

2.5 When must an IFTI report be submitted?

An IFTI report must be reported to AUSTRAC within 10 business days after the day on which the instruction was sent or received.

2.6 What happens if the IFTI report is submitted late or not reported at all?

If the IFTI report is submitted after the 10 business day period or not submitted at all, the AUSTRAC CEO has the power to issue an infringement notice which may request the RE to take specified action to remedy the contravention.

However, depending on the circumstances, the AUSTRAC CEO may apply for a civil penalty order of up to 100,000 penalty units for a body corporate, and up to 20,000 penalty for a person other than a body corporate.

2.7 Who is exempt from IFTI reporting?

There are currently no exemptions for reporting IFTIs. The AUSTRAC CEO does, however, have the capacity to make AML/CTF Rules exempting IFTIs of a specified kind or sent in specified circumstances from the reporting obligation.

2.8 How does an IFTI have to be reported?

If an IFTI is identified it must be reported to the AML/CTF Compliance Officer who will prepare, lodge and retain records of IFTI reporting.

The AML/CTF Compliance Officer will submit IFTI reports to AUSTRAC electronically via AUSTRAC Online.

If circumstances arise where Shinyuan is unable to use AUSTRAC Online (for technical reasons or otherwise) it will obtain and submit the IFTI paper form developed by AUSTRAC. Paper forms can be obtained by calling the AUSTRAC Help Desk on 1300 021 037.

An IFTI report must also contain the reportable details specified in the AML/CTF chapters 16 and 17 of the AML/CTF Rules, set out below:

Reportable details for international funds transfer instructions (items 1 and 2 in section 46)

Instructions transmitted out of Australia

A report about an international funds transfer instruction (the instruction), within the meaning of item 1 of the table in section 46 of the AML/CTF Act, must contain:

- (1) for an instruction within the meaning of paragraph 70(c) of the AML/CTF Act – the complete payer information under section 71 of the AML/CTF Act;
- (2) for an instruction within the meaning of paragraphs 70(a) or 70(b) of the AML/CTF Act – the tracing information under section 72 of the AML/CTF Act;
- (3) the name or identity of the ordering institution;
- (4) where applicable, the name or identity of any branch or department of the ordering institution which the payer requested to transmit the instruction;
- (5) the name or identity of the institution (the sender) transmitting the instruction to the beneficiary institution, if different from subparagraph (3);
- (6) where applicable, the name or identity of the sender's branch or department which transmitted the instruction, if different from subparagraph (4);
- (7) the date on which the sender transmits, or is to transmit, the instruction to the beneficiary institution;
- (8) the name or identity of the beneficiary institution;
- (9) the name or identity of the branch or department of the beneficiary institution at which the funds will be made available to the payee;
- (10) the name of the payee;
- (11) one or more of the following details:
 - (a) the number of any account held by the payee with the beneficiary institution through which the transferred money is to be made available to the payee;
 - (b) the payee's full business or residential address (not being a post box address);
 - (c) where applicable, the type and number of identification relating to the payee;
- (12) the following details as appear in the instruction:
 - (a) any information or directions provided by the payer to the payee in relation to the instruction;

- (b) the name or identity of any interposed institution in the funds transfer chain;
 - (c) the name or identity and account number of any institution through which the beneficiary institution will be reimbursed;
 - (d) any information or directions provided by the ordering institution or interposed institution to another institution in the funds transfer chain under subsection 64(2) of the AML/CTF Act;
 - (e) any other details relating to the instruction;
- (13) the amount referred to in the instruction;
- (14) the currency of the amount referred to in the instruction; and
- (15) the date on which the transferred money becomes available to the payee.

Instructions transmitted into Australia

A report about an international funds transfer instruction (the instruction), within the meaning of item 2 of the table in section 46 of the AML/CTF Act, must contain:

- (1) the name of the payer;
- (2) the name or identity of the institution (the sender) transmitting the instruction to the beneficiary institution;
- (3) the following details as appear in the instruction:
 - (a) for an instruction within the meaning of paragraph 70(c) of the AML/CTF Act:
 - (i) one of the following:
 - (A) the payer’s full business or residential address (not being a post box address);
 - (B) a unique identification number given to the payer by the Commonwealth or an authority of the Commonwealth (for example, an Australian Business Number or an Australian Company Number);
 - (C) a unique identification number given to the payer by the government of a foreign country;
 - (D) the identification number given to the payer by the ordering institution;
 - (E) if the payer is an individual—the payer’s date of birth, the country of the payer’s birth and the town, city or locality of the payer’s birth;

- (ii) if the money is, or is to be, transferred from a single account held by the payer with the ordering institution in Australia—the account number for the account;
- (iii) if subparagraph (3)(a)(ii) does not apply—either:
 - (A) a unique reference number for the transfer instruction; or
 - (B) if the money is, or is to be, transferred from a single account held by the payer with the ordering institution—the account number for the account;
- (b) for an instruction within the meaning of paragraph 70(a) or 70(b) of the AML/CTF Act – the tracing information under section 72 of the AML/CTF Act;
- (c) the name or identity of the ordering institution, if different from subparagraph (2);
- (d) where applicable, the name or identity of any branch or department of the ordering institution which the payer requested to transmit the instruction, if different from subparagraph (3)(e);
- (e) where applicable, the name or identity of the sender’s branch or department which transmitted the instruction;
- (f) the identification code assigned to the instruction by the sender;
- (g) the name or identity of the beneficiary institution;
- (h) the name or identity of any branch or department of the beneficiary institution at which the funds will be made available to the payee;
- (i) the date on which the beneficiary institution received the instruction;
- (j) the name of the payee;
- (k) the payee’s full business or residential address (not being a post box address);
- (l) the number of any account held by the payee with the beneficiary institution through which the transferred money is to be made available to the payee;
- (m) the name or identity of any interposed institution in the funds transfer chain;
- (n) the name or identity and account number of any institution through which the beneficiary institution will be reimbursed;
- (o) any information or directions provided by the payer to the payee in relation to the instruction;
- (p) any information or directions provided by the ordering institution or interposed institution to another institution in the funds transfer chain under subsection 64(2) of the AML/CTF Act;

- (q) any other details relating to the instruction;
- (4) the amount referred to in the instruction;
- (5) the currency of the amount referred to in the instruction; and
- (6) the date on which the transferred money becomes available to the payee.

Reportable details for international funds transfer instructions under a designated remittance arrangement (items 3 and 4 in section 46)

Instructions transmitted out of Australia

A report about an international funds transfer instruction (the instruction), within the meaning of item 3 of the table in section 46 of the AML/CTF Act, must contain:

- (1) if the transferor entity is an individual:
 - (a) the transferor entity's full name;
 - (b) any other name used by the transferor entity, if known;
 - (c) the transferor entity's date of birth;
 - (d) the transferor entity's full residential address (not being a post box address);
 - (e) the transferor entity's postal address, if different from subparagraph (1)(d), if known;
 - (f) the transferor entity's telephone number, if known;
 - (g) the transferor entity's email address, if known;
 - (h) the transferor entity's occupation, business or principal activity and ABN, if known;
 - (i) a description of the reliable and independent documentation and/or electronic data source(s) relied upon to verify the identity of the transferor entity, if applicable;
 - (j) the identification number assigned to the transferor entity, if applicable;
- (2) if the transferor entity is a non-individual:
 - (a) the name of the transferor entity and any business name under which the transferor entity is operating;
 - (b) a description of the legal form of the transferor entity and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (c) the business or principal activity of the transferor entity, if known;
 - (d) the full address (not being a post box address) of the transferor entity at which the entity carries on business, or its principal place of business;
 - (e) the transferor entity's postal address, if different from subparagraph (2)(d), if known;
 - (f) where the transferor entity has an ACN or ARBN – that number;

- (g) where the transferor entity has an ABN – that number;
 - (h) the transferor entity's telephone number, if known;
 - (i) the transferor entity's email address, if known;
 - (j) a description of the reliable and independent documentation and/or electronic data source(s) relied upon to verify the identity of the transferor entity, if applicable;
 - (k) the identification number assigned to the transferor entity, if applicable;
- (3) the name and address (not being a post box address) of a person that accepts money or property from the transferor entity, which is, or is to be, transferred under a designated remittance arrangement;
 - (4) the date on which the person accepts the money or property from the transferor entity;
 - (5) the name, identifier (if applicable) and address (not being a post box address) of the person at which it accepts the instruction from the transferor entity, if different from subparagraph (3);
 - (5A) the number of the transferor entity's account held with the person which accepts the instruction from the transferor entity, if applicable;
 - (6) where a person (other than the person referred to in subparagraph (3)) transmits the instruction for the transfer of money or property under the designated remittance arrangement (transmitter):
 - (a) if the transmitter is an individual:
 - (i) the transmitter's full name;
 - (ii) any other name used by the transmitter, if known;
 - (iii) the transmitter's date of birth, if known;
 - (iv) the transmitter's address (not being a post box address);
 - (v) the transmitter's postal address, if different from subparagraph (6)(a)(iv), if known;
 - (vi) the transmitter's telephone number, if known;
 - (vii) the transmitter's email address, if known;
 - (viii) the transmitter's occupation, business or principal activity, if known;
 - (b) if the transmitter is a non-individual:
 - (i) the name of the transmitter and any business name under which the transmitter is operating;

- (ii) a description of the legal form of the transmitter and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (iii) the business or principal activity of the transmitter, if known;
 - (iv) the address (not being a post box address) of the transmitter at which the transmitter carries on business, or its principal place of business;
 - (v) the transmitter's postal address, if different from subparagraph (6)(b)(iv), if known;
 - (vi) where the transmitter has an ACN or ARBN – that number;
 - (vii) where the transmitter has an ABN – that number;
 - (viii) the transmitter's telephone number, if known;
 - (ix) the transmitter's email address, if known;
- (6A) the name and address of the person in the foreign country to which the transmitter sent the instruction for the transfer of money or property;
- (7) the name, identifier (if applicable) and address of a person (disbursing entity) at which the money or property is, or is to be, made available to the ultimate transferee entity;
- (8) the date on which the money or property becomes accessible for the disbursing entity to make available to the ultimate transferee entity, if known;
- (9) if the ultimate transferee entity is an individual, the ultimate transferee entity's:
- (a) full name;
 - (b) date of birth, if known;
 - (c) address (not being a post box address);
 - (d) postal address, if different from subparagraph (9)(c), if known;
 - (e) telephone number, if known;
 - (f) email address, if known;
- (10) if the ultimate transferee entity is a non-individual:
- (a) the name of the ultimate transferee entity and any business name under which the ultimate transferee entity is operating;
 - (b) a description of the legal form of the ultimate transferee entity and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (c) the business or principal activity of the ultimate transferee entity, if known;

- (d) the address (not being a post box address) of the ultimate transferee entity at which it carries on business, or its principal place of business;
 - (e) the ultimate transferee entity's postal address if different from subparagraph (10)(d), if known;
 - (f) the ultimate transferee entity's telephone number, if known;
 - (g) the ultimate transferee entity's email address, if known;
- (11) if money is to be transferred:
- (a) the amount referred to in the instruction;
 - (b) the currency of the amount referred to in the instruction;
- (12) if property is to be transferred (transferred property):
- (a) a description of the transferred property referred to in the instruction;
 - (b) the value of the transferred property referred to in the instruction;
 - (c) the currency used to value the transferred property referred to in the instruction;
- (12A) if money is to be made available to the ultimate transferee entity by a person in a foreign country depositing or arranging for the money to be deposited into an account held by the ultimate transferee entity with that person, whether or not held jointly with any other person or persons:
- (a) the account number of that account, if applicable;
 - (b) the name in which the account is held, if applicable; and
 - (c) the name and location of the institution at which the account is held;
- (12B) any reference number allocated by the reporting entity to the instruction;
- (13) any information given in the instruction about the reason for transferring the money or property.

Instructions transmitted into Australia

A report about an international funds transfer instruction (the instruction), within the meaning of item 4 in the *table* in section 46 of the AML/CTF Act, must contain:

- (1) if the transferor entity is an individual:
 - (a) the transferor entity's name;
 - (b) any other name used by the transferor entity, if known;
 - (c) the transferor entity's date of birth, if known;

- (d) the transferor entity's address (not being a post box address);
 - (e) the transferor entity's postal address, if different from subparagraph (1)(d), if known;
 - (f) the transferor entity's telephone number, if known;
 - (g) the transferor entity's email address, if known;
 - (h) the transferor entity's occupation, business or principal activity, if known;
- (2) if the transferor entity is a non-individual:
- (a) the name of the transferor entity and any business name under which the transferor entity is operating;
 - (b) a description of the legal form of the transferor entity and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (c) the business or principal activity of the transferor entity, if known;
 - (d) the address (not being a post box address) of the transferor entity at which it carries on business, or its principal place of business;
 - (e) the transferor entity's postal address, if different from subparagraph (2)(d), if known;
 - (f) the transferor entity's telephone number, if known;
 - (g) the transferor entity's email address, if known;
- (3) for a person in a foreign country who accepts the instruction from the transferor entity for the transfer of money or property (foreign entity):
- (a) if the foreign entity is an individual:
 - (i) the foreign entity's full name;
 - (ii) any other name used by the foreign entity, if known;
 - (iii) the foreign entity's date of birth, if known;
 - (iv) the foreign entity's address (not being a post box address);
 - (v) the foreign entity's postal address, if different from subparagraph (3)(a)(iv), if known;
 - (vi) the foreign entity's telephone number, if known;
 - (vii) the foreign entity's email address, if known;
 - (viii) the foreign entity's occupation, business or principal activity, if known;

- (b) if the foreign entity is a non-individual:
 - (i) the name of the foreign entity and any business name under which the foreign entity is operating;
 - (ii) a description of the legal form of the foreign entity and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (iii) the business or principal activity of the foreign entity, if known;
 - (iv) the address (not being a post box address) of the foreign entity at which it carries on business, or its principal place of business;
 - (v) the foreign entity's postal address, if different from subparagraph (3)(b)(iv), if known;
 - (vi) the foreign entity's telephone number, if known;
 - (vii) the foreign entity's email address, if known;
- (4) the date on which the foreign entity accepts the money or property from the transferor entity;
- (5) the name, identifier (if applicable) and address (not being a post box address) of the foreign entity at which it accepts the instruction from the transferor entity, if applicable and known;
- (5A) the number of the transferor entity's account held with the foreign entity which accepts the instruction from the transferor entity, if applicable;
- (6) where a person (other than the foreign entity) transmits the instruction for the transfer of money or property under the designated remittance arrangement (transmitter):
 - (a) if the transmitter is an individual:
 - (i) the transmitter's full name, if known;
 - (ii) any other name used by the transmitter, if known;
 - (iii) the transmitter's date of birth, if known;
 - (iv) the transmitter's address (not being a post box address), if known;
 - (v) the transmitter's postal address, if different from subparagraph (6)(a)(iv), if known;
 - (vi) the transmitter's telephone number, if known;
 - (vii) the transmitter's email address, if known;
 - (viii) the transmitter's occupation, business or principal activity, if known;
 - (b) if the transmitter is a non-individual:

- (i) the name of the transmitter and any business name under which the transmitter is operating, if known;
 - (ii) a description of the legal form of the transmitter and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (iii) the business or principal activity of the transmitter, if known;
 - (iv) the address (not being a post box address) of the transmitter at which it carries on business, or its principal place of business, if known;
 - (v) the transmitter's postal address, if different from subparagraph (6)(b)(iv), if known;
 - (vi) the transmitter's telephone number, if known;
 - (vii) the transmitter's email address, if known;
- (6A) the name and address of the entity in Australia to which the instruction for the transfer of money or property was sent by the transmitter;
- (7) the date on which the reporting entity makes or will make the money or property available to the ultimate transferee entity;
- (8) the name and full address (not being a post box address) of the reporting entity that makes or will make the money or property available to the ultimate transferee entity in Australia;
- (9) the name, identifier (if applicable) and address (not being a post box address) of the reporting entity, if different from subparagraph (8), at which the money or property was made or is to be made available to the ultimate transferee entity in Australia;
- (10) if the ultimate transferee entity is an individual, the ultimate transferee entity's:
- (a) full name;
 - (b) date of birth, if known;
 - (c) full residential address (not being a post box address), if known;
 - (d) postal address, if different from subparagraph (10)(c), if known;
 - (e) telephone number, if known;
 - (f) email address, if known;
 - (g) occupation, business or principal activity and ABN, if known;
- (11) if the ultimate transferee entity is a non-individual:

- (a) the name of the ultimate transferee entity and any business name under which the ultimate transferee entity is operating;
 - (b) a description of the legal form of the ultimate transferee entity and any business structure it is a part of, for the purposes of its main business activities, if known (for example, partnership, trust or company);
 - (c) the business or principal activity of the ultimate transferee entity, if known;
 - (d) the full address (not being a post box address) of the ultimate transferee entity at which it carries on business, or its principal place of business, if known;
 - (e) the ultimate transferee entity's postal address, if different from subparagraph (11)(d), if known;
 - (f) where the ultimate transferee entity has an ACN or ARBN – that number;
 - (g) where the ultimate transferee entity has an ABN – that number;
 - (h) the ultimate transferee entity's telephone number, if known;
 - (i) the ultimate transferee entity's email address, if known;
- (12) if money is to be transferred:
- (a) the amount referred to in the instruction;
 - (b) the currency of the amount referred to in the instruction;
- (13) if property is to be transferred (transferred property):
- (a) a description of the transferred property referred to in the instruction;
 - (b) the value of the transferred property referred to in the instruction;
 - (c) the currency used to value the transferred property referred to in the instruction;
- (13A) if money is to be made available to the ultimate transferee entity by a person in Australia depositing or arranging for the money to be deposited into an account held by the ultimate transferee entity with that person, whether or not held jointly with any other person or persons:
- (a) the account number of that account, if applicable;
 - (b) the name in which the account is held, if applicable; and
 - (c) the name and location of the institution at which the account is held;
- (13B) any reference number allocated by the reporting entity to the instruction;
- (14) any information given in the instruction about the reason for transferring the money or property.

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

- (1) Full name;
- (2) Job title or position;
- (3) Telephone number; and
- (4) Email address.