



Anti-Money Laundering and Counter-Terrorism Financing Program

Introduction and Part A

iTeller Pty Ltd

TABLE OF CONTENTS

INTRODUCTION	4
1. ABOUT THE AML/CTF ACT	4
2. ADOPTION.....	4
3. RECORDS RELATING TO ITELLER'S AML/CTF PROGRAM	4
4. AUSTRAC ENROLMENT AND REGISTRATION.....	5
5. PENALTIES.....	6
6. DESIGNATED BUSINESS GROUP	6
7. DEFINITIONS.....	7
8. PURPOSE AND APPLICATION OF PART A.....	13
9. OVERSIGHT BY THE DIRECTOR AND DIRECTOR'S APPROVAL	13
10. ITELLER'S AML/CTF COMPLIANCE OFFICER.....	14
11. REVIEW OF THE PROGRAM.....	15
12. AUSTRAC FEEDBACK	19
13. WHAT IS MONEY LAUNDERING?.....	19
14. WHAT IS TERRORISM FINANCING?.....	20
15. DESIGNATED SERVICES PROVIDED BY ITELLER	21
16. RISK ASSESSMENT AND MANAGEMENT MATRIX.....	23

17. EMPLOYEE DUE DILIGENCE PROGRAM.....	24
18. RISK AWARENESS TRAINING PROGRAM.....	27
19. OUTSOURCING.....	28
20. PROVISION OF DESIGNATED SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES	30
21. RELIANCE ON THIRD PARTY CUSTOMER IDENTIFICATION PROCEDURES	30
22. RECORD KEEPING OBLIGATIONS RELATING TO CUSTOMER IDENTIFICATION AND THE PROVISION OF DESIGNATED SERVICES	31
23. TRANSACTION MONITORING.....	32
24. SUSPICIOUS MATTER REPORTING	34
25. TRANSACTION REPORTING - THRESHOLD TRANSACTION REPORTS	40
26. TRANSACTION REPORTING - INTERNATIONAL FUNDS TRANSFER INSTRUCTION REPORTS – INTERNATIONAL FUNDS TRANSFER INSTRUCTION UNDER A DESIGNATED REMITTANCE ARRANGEMENT	42
27. AML/CTF COMPLIANCE REPORTS	45
28. CHANGES TO OUR AUSTRAC ENROLMENT/REGISTRATION DETAILS	45
29. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER	46
30. ONGOING CUSTOMER DUE DILIGENCE	46

INTRODUCTION

1. ABOUT THE AML/CTF ACT

- 1.1 The *Anti-Money Laundering (“**AML**”) and Counter-Terrorism Financing (“**CTF**”) Act 2006 (“**AML/CTF Act**”)*’s and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (“**Rules**”)* broad purpose is to regulate financial transactions in a way that will help identify, mitigate and manage money laundering and terrorism financing risks.
- 1.2 The AML/CTF Act provides general principles and obligations while detailed operating rules are covered in rules made by the Australian Transaction Reports and Analysis Centre (“**AUSTRAC**”). AUSTRAC is the government agency responsible for administering the AML/CTF Act.
- 1.3 The AML/CTF Act applies to persons who provide specified services (known as “**designated services**”). Persons providing designated services are called “reporting entities”.
- 1.4 iTeller Pty Ltd (“**iTeller**”) provides one or more designated services listed in the AML/CTF Act and is therefore a reporting entity. These services are included in the AML/CTF Act because they are vulnerable to abuse by criminals for money laundering or terrorism financing purposes.
- 1.5 The AML/CTF Act adopts a risk-based approach. This approach means that the reporting entity decides how best to identify, mitigate and manage the risk of money laundering and terrorism financing through its business. Reporting entities therefore need to undertake a comprehensive assessment of these risks relative to their businesses. Reporting entities need to be able to demonstrate to AUSTRAC that they have carried out such an assessment and have a documented program in place to identify, mitigate and manage the risk of their products or services being used to facilitate money laundering or terrorism financing.

2. ADOPTION

- 2.1 iTeller adopts Parts A and B of this Program as its AML/CTF Program (“**Program**”) for the purposes of the AML/CTF Act on and from 27 June 2023. iTeller must comply with the Program, as varied from time to time.

VERSION NUMBER	DATE UPDATED	NOTES
1	27 June 2023	Original document prepared and finalised.

3. RECORDS RELATING TO ITELLER’S AML/CTF PROGRAM

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

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

3.2 The records referred to in Section 3.1 of this Program are be retained:

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

4. AUSTRAC ENROLMENT AND REGISTRATION

4.1 iTeller is enrolled and registered with AUSTRAC as an Independent Remittance Dealer and a Digital Currency Exchange Provider.

4.2 Independent Remittance Dealers and Digital Currency Exchange Providers are required to enrol **and** register with AUSTRAC. Enrolling and registering are separate legal requirements and both must be completed.

ENROLLING WITH AUSTRAC	
Responsible Person	AML/CTF CO
Timeframe	iTeller must enrol within twenty-eight (28) days of providing or commencing to provide a designated service.

Changes to Enrolment	Enrolment details must be kept up to date and AUSTRAC must be notified within fourteen (14) days of any changes to iTeller's details. For further information refer to Section 22.4 of Part A.
REGISTERING WITH AUSTRAC	
Responsible Person	AML/CTF CO
Timeframe	Prior to providing or commencing to provide a designated service. A Registrable Digital Currency Exchange Service must not be provided if iTeller has not registered with AUSTRAC. Failure to register may constitute the commission of a criminal offence.
Changes to Registration	Registration details must be kept up to date and AUSTRAC must be notified within fourteen (14) days of any changes to iTeller's details. For further information refer to Section 27 of Part A.

5. PENALTIES

- 5.1 Failure to comply with the obligations under the AML/CTF Act may result in civil or criminal penalties.
- 5.2 Civil penalties for contravention of the AML/CTF Act range up to \$3.4 million for an individual and up to \$17 million for a corporation.
- 5.3 The penalties for criminal offences include imprisonment for up to ten (10) years and/or fines up to \$1.7 million.

6. DESIGNATED BUSINESS GROUP

- 6.1 iTeller is a reporting entity which 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.
- 6.2 Another entity can join with iTeller to form iTeller's DBG if:
 - (a) that entity is:
 - (i) related to each other member of iTeller's DBG within the meaning of section 50 of the *Corporations Act 2001*;

(ii) either:

- A. a reporting entity;
- B. a company in a foreign country which if it were resident in Australia would be a reporting entity; or
- C. providing a designated service pursuant to a joint venture agreement, to which each member of iTeller's DBG is a party; and

(iii) not a member of another DBG; or

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

6.3 In order to join iTeller's DBG, a director or officer of the other entity needs to elect in writing (on behalf of that entity) to be a member of iTeller's DBG by completing the election form as specified by AUSTRAC at the time. The AML/CTF CO provides the completed form to AUSTRAC in the method specified by AUSTRAC.

6.4 When any of the following changes in iTeller's DBG occurs, the AML/CTF CO must notify AUSTRAC's CEO, in writing, by completing the approved notification form:

- (a) a withdrawal of a member from iTeller's DBG;
- (b) an election of a new member to join iTeller's DBG;
- (c) the termination of iTeller's DBG; or
- (d) any other change in the details previously notified to AUSTRAC's CEO in respect of the Nominated Contact Officer or iTeller's DBG.

6.5 Any of the changes listed in Section 6.4 of the Program must be approved by the Director of iTeller.

6.6 The AML/CTF CO must provide the notification to AUSTRAC no later than fourteen (14) business days from the date the change takes effect.

7. DEFINITIONS

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

DEFINITIONS	
Australian Government Entity	<ul style="list-style-type: none"> (a) the Commonwealth, a State or a Territory; or (b) an agency or authority of: <ul style="list-style-type: none"> (i) the Commonwealth; or (ii) a State; or (iii) a local governing body established by or under a law of the Commonwealth, a State or Territory, other than a body whose sole or principal function is to provide a particular service, such as the supply of electricity or water.
Authorised Officer	in accordance with section 5 of the AML/CTF Act, an authorised officer is 'the AUSTRAC CEO or a person for whom an appointment as an authorised officer is in force under section 145'.
Beneficial Owner	<ul style="list-style-type: none"> (a) of a person who is a reporting entity, means an individual who owns or controls (directly or indirectly) the reporting entity; (b) of a person who is a customer of a reporting entity, means an individual who ultimately owns or controls (directly or indirectly) the customer; (c) in this definition, control includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies; and (d) in this definition, owns means ownership (either directly or indirectly) of 25% or more of a person.
Digital Currency	<ul style="list-style-type: none"> (a) a digital representation of value that: <ul style="list-style-type: none"> (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

	<ul style="list-style-type: none"> (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 <p>(b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;</p> <p>(c) but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of this Act.</p>
Digital Currency Exchange Provider	means a person running a business that exchanges digital currency with money or vice versa.
Independent Remittance Dealer	means businesses which provide remittance services directly to customers using their own systems and processes. Typically, transfers for customers are conducted through the business's bank accounts rather than through a system provided by a registered Remittance Network Provider.
Politically Exposed Persons ("PEP")	<p>means an individual:</p> <ul style="list-style-type: none"> (a) who holds a prominent public position or function in a government body or an international organisation, including: <ul style="list-style-type: none"> (i) Head of State or head of a country or government; or (ii) government minister or equivalent senior politician; or (iii) senior government official; or (iv) Judge of the High Court of Australia, the Federal Court of Australia or a Supreme Court of a State or Territory, or a Judge of a court of equivalent seniority in a foreign country or international organisation; or (v) governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of Australia; or (vi) senior foreign representative, ambassador, or high commissioner; or (vii) high-ranking member of the armed forces; or

	<p>(viii) board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise or international organisation; and</p> <p>(b) who is an immediate family member of a person referred to in paragraph (a), including:</p> <ul style="list-style-type: none"> (i) a spouse; or (ii) a de facto partner; or (iii) a child and a child's spouse or de facto partner; or (iv) a parent; and <p>(c) who is a close associate of a person referred to in paragraph (b), which means any individual who is known (having regard to information that is public or readily available) to have:</p> <ul style="list-style-type: none"> (i) joint beneficial ownership of a legal entity or legal arrangement with a person referred to in paragraph (b); or (ii) sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph (b). <p>(d) In this Program:</p> <ul style="list-style-type: none"> (i) domestic politically exposed person means a politically exposed person of an Australian government body; (ii) foreign politically exposed person means a politically exposed person of a government body of a foreign country; (iii) international organisation politically exposed person means a politically exposed person of an international organisation. <p>(e) In this definition international organisation means an organisation:</p> <ul style="list-style-type: none"> (i) established by formal political agreement by two or more countries and that agreement has the status of an international treaty; and (ii) recognised in the law of the countries which are members of the organisation.
--	--

Primary Non-Photographic Identification Document	<ul style="list-style-type: none"> (a) a birth certificate or birth extract issued by a State or Territory; (b) a citizenship certificate issued by the Commonwealth; (c) a citizenship certificate issued by a foreign government that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator; (d) a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator; or (e) a concession card, as defined from time to time in the Social Security Act 1991, or an equivalent term which expresses the same concept in relation to concession holders.
Primary Photographic Identification Document	<ul style="list-style-type: none"> (a) a licence or permit issued under a law of a State or Territory or equivalent authority of a foreign country for the purpose of driving a vehicle that contains a photograph of the person in whose name the document is issued; (b) a passport issued by the Commonwealth; (c) a passport or a similar document issued for the purpose of international travel, that: <ul style="list-style-type: none"> (i) contains a photograph and either: <ul style="list-style-type: none"> A. the signature of the person in whose name the document is issued; or B. any unique identifier of the person in whose name the document is issued; (ii) is issued by a foreign government, the United Nations or an agency of the United Nations; and (iii) if it is written in a language that is not understood by the person carrying out the verification - is accompanied by an English translation prepared by an accredited translator; (d) a card issued under a law of a State or Territory for the purpose of proving the person's age which contains a photograph of the person in whose name the document is issued; (e) a national identity card issued for the purpose of identification, that: <ul style="list-style-type: none"> (i) contains a photograph and either:

	<p>A. the signature of the person in whose name the document is issued; or</p> <p>B. any unique identifier of the person in whose name the document is issued;</p> <p>(ii) is issued by a foreign government, the United Nations or an agency of the United Nations; and</p> <p>(iii) if it is written in a language that is not understood by the person carrying out the verification - is accompanied by an English translation prepared by an accredited translator.</p>
Reasonable Measures	means appropriate measures which are commensurate with the money laundering or terrorism financing risks.
Registrable Designated Remittance Services	<p>means a designated service that:</p> <p>(a) is covered by item 31, 32, 32A and 50 of table 1 in section 6; and</p> <p>(b) is provided by a person at or through a permanent establishment of the person in Australia; and</p> <p>(c) is not of a kind specified in the AML/CTF Rules.</p>
Registrable Digital Currency Exchange Service	<p>means a designated service that:</p> <p>(a) is covered by item 50A of table 1 in section 6 of the AML/CTF Act; and</p> <p>(b) is not of a kind specified in the AML/CTF Rules.</p>
Secondary Identification Document	<p>(a) a notice that:</p> <p>(i) was issued to an individual by the Commonwealth, a State or a Territory within the preceding twelve months;</p> <p>(ii) contains the name of the individual and his or her residential address; and</p> <p>(iii) records the provision of financial benefits to the individual under a law of the Commonwealth, State or Territory (as the case may be);</p> <p>(b) a notice that:</p> <p>(i) was issued to an individual by the Australian Taxation Office within the preceding 12 months;</p> <p>(ii) contains the name of the individual and his or her residential address; and</p>

	<ul style="list-style-type: none"> (iii) records a debt payable to or by the individual by or to (respectively) the Commonwealth under a Commonwealth law relating to taxation; <p>(c) a notice that:</p> <ul style="list-style-type: none"> (i) was issued to an individual by a local government body or utilities provider within the preceding three months; (ii) contains the name of the individual and his or her residential address; and (iii) records the provision of services by that local government body or utilities provider to that address or to that person. <p>(d) in relation to a person under the age of 18, a notice that:</p> <ul style="list-style-type: none"> (i) was issued to a person by a school principal within the preceding three months; (ii) contains the name of the person and his or her residential address; and (iii) records the period of time that the person attended at the school.
--	---

8. PURPOSE AND APPLICATION OF PART A

- 8.1 Part A of this Program (“**Part A**”) is designed to identify, mitigate and manage the money laundering or terrorism financing risk which iTeller Pty Ltd may reasonably face in the provision of our designated services.
- 8.2 Part A applies to all aspects of iTeller’s business, to which the Act and the Rules are applicable and to any functions which are outsourced to third parties.
- 8.3 All iTeller’s staff are given a copy of Part A of this Program and provided with necessary training so they understand the nature and purpose of our business relationship with iTeller’s customers and iTeller’s obligations under the Act and Rules.

9. OVERSIGHT BY THE DIRECTOR AND DIRECTOR’S APPROVAL

- 9.1 Part A of this Program was approved and adopted by iTeller’s Director 27 June 2023.
- 9.2 Part A is subject to ongoing oversight by the Director and iTeller’s AML/CTF CO, and

- (a) The AML/CTF CO, in consultation with senior management, reviews Part A on at least an annual basis to ensure Part A is:
 - (i) drafted in accordance with the AML/CTF Act and Rules;
 - (ii) applicable and relevant to the functions of iTeller's business operations; and
 - (iii) any changes to iTeller's designated services have been reflected in Part A.
 - (b) The review of Part A is presented to the Director at the next Board meeting/meeting of the Director and AML/CTF CO; and
 - (c) Any changes to Part A are required to be reviewed and approved by the Director.
- 9.3 Part B does not require the Director's approval but is subject to ongoing oversight by the Director, senior management and iTeller's AML/CTF CO. Any changes to Part B are required to be reviewed and approved by the AML/CTF CO of iTeller.
- 9.4 Monthly meetings with the Director are held by the AML/CTF CO to report on the following:
- (a) significant changes to the ML or TF risks affecting iTeller;
 - (b) compliance with this Program, the AML/CTF Act and Rules by iTeller;
 - (c) the results of and any report produced for any internal or external review of this Program;
 - (d) assessment of the ML and TF risks associated with any new product, delivery channels, business partners and any operation of iTeller, and whether the existing procedures and controls are appropriate and proportionate to the ML and TF risks;
 - (e) any AUSTRAC feedback; and
 - (f) changes to relevant legislation.

10. ITELLER'S AML/CTF COMPLIANCE OFFICER

- 10.1 iTeller has appointed Ms Shirin Arkvaz, as iTeller's AML/CTF CO for the purposes of the AML/CTF Act and Rules, and also the Nominated Contact Officer for the purposes of the Rules.

- 10.2 Shirin Arkvaz is at all times be part of the management of iTeller, report directly to the Director, and possess sufficient skills and experience to carry out the roles of the AML/CTF CO.
- 10.3 The AML/CTF CO has successfully completed 20 CPD units from the AML/CTF Course by Financial Educational Professionals on 15 April 2023.
- 10.4 The AML/CTF CO is responsible for implementing and over-seeing iTeller's obligations under the AML/CTF Act and Rules in accordance with its compliance procedures, including but not limited to:
- (a) providing regulatory and/or legal updates in relation to the AML/CTF Act and Rules – the AML/CTF CO shall regularly monitor the information circulars AUSTRAC publishes on its website and take such information into account when implementing iTeller's Program;
 - (b) ongoing monitoring of the implementation of the Program;
 - (c) considering and incorporating feedback from employees, clients and AUSTRAC;
 - (d) ensuring overall compliance with the AML/CTF Act and Rules;
 - (e) investigating suspicious matters, issues or incidents in iTeller's operation which may give rise to ML/TF risks;
 - (f) maintaining records; and
 - (g) conducting employee risk awareness training in accordance with iTeller's obligations under the AML/CTF Act and Rules.
- 10.5 The AML/CTF CO is authorised to act independently and to delegate any of their responsibilities under this Program to another iTeller employee, agent or responsible third party provided if it is reasonable to do so. The AML/CTF CO also liaises with iTeller's external compliance consultant.
- 10.6 If iTeller or any employee or representative of iTeller receives correspondence or enquiries from AUSTRAC, those enquiries should be directed to the AML/CTF CO at first instance.

11. REVIEW OF THE PROGRAM

- 11.1 **Internal Reviews:** The AML/CTF CO must regularly assess iTeller's ML and TF risk and should take steps to have this Program modified appropriately.

INTERNAL REVIEWS	
Responsible Person:	AML/CTF CO
Frequency:	Quarterly (unless otherwise indicated based on the factors listed below)
When an internal review must be conducted:	
<p>(a) Where a significant change in the ML or TF risk relating to the designated services provided by iTeller has been identified;</p> <p>(b) prior to iTeller introducing a new designated service to the market;</p> <p>(c) prior to iTeller adopting a new method of delivering a designated service;</p> <p>(d) prior to iTeller adopting a new technology or developing technology used for the provision of an existing or new designated service; and</p> <p>(e) where the AML/CTF CO identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of iTeller's customers.</p> <p>The above issues must also be considered during each independent review.</p>	

11.2 Independent Reviews: The AML/CTF CO must engage an experienced internal or external third party to conduct an independent review of this Program.

INDEPENDENT REVIEWS	
Responsible Person:	AML/CTF CO - report the results of the independent review to the Director of iTeller. Reports detailing the review (both internal and external) and the results provided to the Director for consideration and discussion. The reports then form the basis of a timetable to address the findings within the timeline set by the Director.
Frequency:	Annually
Who should to do the external review?	The independent party conducting the review must be independent and:

	<ul style="list-style-type: none"> (a) have not been involved in undertaking any of the functions or measures required to be carried out under this Program; (b) have not been involved in the design, development, implementation, maintenance or management of this Program; (c) have not been involved in the development of iTeller's risk assessment or related internal controls; (d) have access to the employees of iTeller and is able to make enquiries of any employee; (e) have access to the records, personnel and property of iTeller within the context of iTeller's obligations under the <i>Privacy Act 1988</i>; (f) be impartial and objective in performing their duties and should not be inappropriately influenced by management of iTeller; and (g) be appropriately qualified to conduct the review.
What should be covered in the review?	<p>The independent party, in the course of carrying out the independent review, must:</p> <ul style="list-style-type: none"> (a) assess the effectiveness of Part A having regard to the ML and TF risk of iTeller; (b) assess whether Part A complies with the Rules; (c) assess whether Part A has been effectively implemented; (d) assess whether iTeller has complied with Part A; <p>The independent party, in the course of carrying out the independent review, may also:</p> <ul style="list-style-type: none"> (a) assess the risk management resources available to iTeller including, but not limited to funding and staff allocation; (b) identify any future needs relevant to the nature, size and complexity of iTeller; (c) assess the ongoing risk management procedures and controls in order to identify any failures – the following factors should be taken into account: <ul style="list-style-type: none"> (i) any market information relevant to the global AML/CTF environment which may have an impact on the ML or TF risk faced by iTeller; (ii) failure to include all mandatory legislative components in the Program;

	<ul style="list-style-type: none"> (iii) failure to gain approval for the Program from iTeller's Director; (iv) insufficient or inappropriate employee due diligence; (v) frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s); (vi) changes in business functions which are not reflected in this Program; (vii) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging ML/TF 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: <ul style="list-style-type: none"> A. prompt, if appropriate, for further identification and/or verification to be carried out when the ML/TF 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;
--	---

	<ul style="list-style-type: none"> (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: <ul style="list-style-type: none"> A. customer identification policies, procedures and systems; and B. identifying potential AML/CTF risks; and (xiii) assess the acceptance of documentation that may not be readily verifiable. <p>If the independent reviewer determines it is appropriate, the review may also:</p> <ul style="list-style-type: none"> (a) assess whether the risk-based procedures and processes adopted in iTeller's Program have changed such that alterations need to be made; (b) assess whether Part B is sufficient to cover the ML/TF risks posed by existing and potential customers of iTeller; and (c) assess whether any additional changes need to be made to this Program as a result of changes to the AML/CTF Act and Rules and the AML/CTF environment generally.
--	--

12. AUSTRAC FEEDBACK

- 12.1 Where AUSTRAC provides iTeller with feedback regarding performance in the management of ML/TF risk, any receipt of such feedback is immediately referred to the AML/CTF CO for attention.
- 12.2 The AML/CTF CO assesses AUSTRAC's feedback to determine if any changes to this Program are required and implement any such changes as soon as reasonably practicable with the Director's approval.

13. WHAT IS MONEY LAUNDERING?

- 13.1 Money laundering ("**ML**") is the process used to disguise the illegal origin of the proceeds of illegal activities such as drug trafficking, tax evasion, smuggling, theft, terrorism, arms trafficking and corrupt practices. It is the name given to the process by which illegally obtained funds are given the appearance of having been legitimately obtained.

13.2 Whilst initially there was a focus on cash transactions there has recently been a growth in awareness of the sophistication used by money launderers to structure transactions to prevent detection and investment by them in a range of assets within the financial services sector.

13.3 There are three main stages of ML:

- (a) **Placement** – the physical disposal of the proceeds e.g. deposit into an account. This is usually when illegal funds or assets are first brought into the financial system.
- (b) **Layering** – creating complex layers of financial transactions to separate the proceeds from their source and hide any audit trail to maintain anonymity e.g. transferring investments from one product to another. Many different techniques can be used to layer the funds including use of corporations and trusts. The funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.
- (c) **Integration** – taking the proceeds of ML and placing them back into the financial system so that they appear to be normal business proceeds with apparent legitimacy e.g. settling money into a trust without links to the previous illicit funds with the trust then making investments.

14. WHAT IS TERRORISM FINANCING?

14.1 Terrorism financing (“TF”) is often the reverse of ML whereby funds within a legitimate source are put into the financial system and redirected into the hands of terrorist organisations. Where those funds are the proceeds of illegal activities including fraud and criminal activities they may also be captured by AML controls.

14.2 Terrorist organisations obtain money from a number of legitimate and illegitimate sources, such as:

- (a) **Illegal Activities** – terrorists obtain funds from illegal activities, such as drug trafficking, smuggling, kidnapping and extortion.
- (b) **Rich Individuals** - it is increasingly apparent that rich individuals are a critical source of terrorist financing.
- (c) **Charitable and Religious Institutions** – charitable and religious institutions can be a source of terrorist funding. They are ideal conduits because they are very lightly regulated and do not need to provide a commercial justification for their activities.
- (d) **Commercial Enterprise** – terrorist organisations may run or own otherwise legitimate commercial enterprise to generate profits and commingle illegal funds. These include jewellery businesses, trading companies, convenience stores, real estate ventures and investment management firms.

- (e) **State Sponsors** – a number of rogue nations have been known to provide assistance, financial support and safe harbour to terrorist organisations.

15. DESIGNATED SERVICES PROVIDED BY ITELLER

15.1 iTeller provides the following designed services:

- (a) Item 50A of section 6 of the Act.

Digital Currency Exchange

15.2 iTeller deals in the following digital currencies:

- (a) iTeller Coin
- (b) Bitcoin (“**BTC**”)
- (c) Ethereum (“**ETH**”)
- (d) Cardano (“**ADA**”)
- (e) Ripple (“**XRP**”)

iTeller utilises a third-party platform, L-Bank, which enables customers to purchase United States Dollar Tether (“**USDT**”), and subsequently exchange USDT with other cryptocurrency including iTeller Coin.

15.3 iTeller undertakes due diligence on the supply sources of the exchanged digital currencies to ensure they are trusted and reliable. iTeller has a contractual agreement in place between iTeller and L-Bank.

15.4 iTeller offers the following services to customers (as specified in Section 30.2 of this Program):

- (a) Exchanging digital currency from USDT Cryptocurrency to iTeller Coin;
- (b) Exchanging digital currencies into physical currencies through the use of an Automated Teller Machine (“**ATM**”); and

- (c) Exchanging physical currencies into digital currencies through the use of an ATM.

15.5 iTeller has undertaken assessment of the ML/TF risks associated with its designated services taking into account the following factors:

- (a) nature, size and complexity of its business;
- (b) type of ML/TF risk that iTeller might reasonably face;
- (c) customer types, including any politically exposed persons;
- (d) types of designated services provided;
- (e) methods by which those services are delivered;
- (f) jurisdictions in which those services are delivered;
- (g) responsible third parties to whom iTeller outsource its AML/CTF obligations;
- (h) any significant changes in ML/TF risk;
- (i) any ML/TF risk posed by:
 - (i) new designated services – the assessment is conducted prior to the introduction of the new designated services;
 - (ii) new delivery method - the assessment is conducted prior to the introduction of the new delivery method; and
 - (iii) new or developing technologies used in the provision of the designated services - the assessment is conducted prior to the introduction of the new technologies.

15.6 **Significant Changes to the Customer's Business:** if iTeller notices that any of the following significant changes to the customer's business have taken place, iTeller will obtain further details in writing from the customer to satisfy itself that the customer does not present an unacceptable risk. Significant changes can be identified as one of the following:

- (a) changes in the nature of the customer's business or business relationship;

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

- 15.7 **New Designated Services:** prior to a new service being introduced to the market by iTeller, the AML/CTF CO assesses it to determine whether it involves the provision of a designated service. When it is determined by the AML/CTF CO that a new service involves the provision of a designated service, the AML/CTF CO assesses the ML/TF risk involved in the provision of the new designated service.
- 15.8 Board approval must be received before a new designated service is introduced to the market. The Board must be given a copy of the risk assessment conducted before the approval is granted.

16. RISK ASSESSMENT AND MANAGEMENT MATRIX

- 16.1 iTeller has put in place a Risk Assessment and Management Matrix ("**AML/CTF Matrix**") which outlines our assessment of various ML/TF risks associated with our designated services and the measures we put in place to control such risks. The AML/CTF Risk Matrix is attached at Annexure A of the Program.
- 16.2 The Risk Assessment and Management Matrix is reviewed by the AML/CTF Co on a monthly basis.

RISK ASSESSMENT AND MANAGEMENT MATRIX	
Responsible Person:	AML/CTF CO - review and update the AML/CTF Matrix to ensure that the following items are contained in the AML/CTF Matrix and updated regularly.
Risk identification of the main ML/TF risks:	<ul style="list-style-type: none"> (a) Customer types (b) Products & services (c) Business practices & delivery methods (d) Countries we deal with

Risk Assessment / Measurement of the risk:	<ul style="list-style-type: none"> (a) Likelihood – chance of risking happening (b) Impact – the amount of loss or damage if the risk is to occur (c) Likelihood x impact – the level of risk or risk score
Mitigating and managing the risk:	<ul style="list-style-type: none"> (a) Minimise and manage the risks (b) Application of strategies, policies and procedures (c) Existing systems and controls (d) Risk plan
Risk Monitoring and Review:	<ul style="list-style-type: none"> (a) Development and implementation of monitoring process (b) Record keeping (c) Review of risk plan and this Program (d) Independent review

17. EMPLOYEE DUE DILIGENCE PROGRAM

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

17.2 New Employees

- (a) The AML/CTF CO must be informed of all prospective new employees before they are issued with an employment contract with iTeller. The prospective employee will be informed that their employment is subject to the result of their background checks.
- (b) The AML/CTF CO must undertake a risk assessment for all newly created roles or previously existing roles that are to be filled with a new employee to determine whether they will be in a position to facilitate the commission of a ML/TF offence. iTeller determines the prospective employee's suitability for the role by assessing them against a list of objective benchmarks that must be met before they are appointed to the role.

- (c) For all new employees, regardless of their position, iTeller must carry out all of the following checks, prior to an offer of employment being made:
- (i) collect and verify their identification documents as if they are a new client;
 - (ii) obtain a copy of their working visa (where the employee is not an Australian citizen);
 - (iii) confirm employment history;
 - (iv) carry out at least two (2) reference checks;
 - (v) obtain copies of all tertiary educational qualifications or if none, the person's highest educational qualification;
 - (vi) carry out a criminal history check with the Australian Federal Police (“**AFP**”);
 - (vii) carry out a bankruptcy/credit check;
 - (viii) Australian Securities and Investments Commission (“**ASIC**”) Banned and Disqualified Persons Check;
 - (ix) ASIC enforceable undertaking register check;
 - (x) Sanctions and PEP checks;
 - (xi) Adverse media check;
 - (xii) Check to confirm if the new employee has lived in a high-risk jurisdiction; and
 - (xiii) Check to confirm if the new employee has been subject to regulatory, court or legal action.
- (d) iTeller will perform document verification service checks upon potential employees. As iTeller is required under the AML/CTF Act to obtain consent from an individual prior to collecting personally identifiable information, iTeller will obtain written consent from the individual that they agree to their identifying information being checked with the issuer or official record holder.
- (e) If iTeller determines the results to any of these procedures are not satisfactory, iTeller will not offer that person employment. Results which are not satisfactory may include:

- (i) a criminal history check which returns a result including fraud, dishonest conduct or other ML/TF offences;
- (ii) the prospective employee is currently bankrupt;
- (iii) the prospective employee does not hold a valid working visa;
- (iv) the identity of the prospective employee cannot be verified; or
- (v) the references obtained by iTeller uncover evidence that the prospective employee has been involved in activities which may constitute an ML/TF risk to iTeller.

17.3 Existing Employees

- (a) Where iTeller proposes to transfer or promote an existing employee 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/TF offence. iTeller determines the employee's suitability for the role by assessing their performance against a list of objective benchmarks or performance indicators that must be met before they are appointed to the new role.
- (b) Where an employee is transferred or promoted to a role that may put them in a position to facilitate the commission of a ML/TF offence in connection with the provision of a designated service, the AML/CTF CO will:
 - (i) obtain an updated copy of the employee's working visa (where the employee is not an Australian citizen);
 - (ii) carry out any other identification, reference, criminal history checks with the AFP, bankruptcy or credit checks that are deemed necessary by the AML/CTF CO; and
 - (iii) assesses the employee's suitability for the role against a list of objective benchmarks or performance indicators.
- (c) Employees who fail to comply with the procedures above will be reported to iTeller's Director Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

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

17.5 Managing Non-Compliance

- (a) iTeller will, on an ongoing basis, monitor compliance with this Program.
- (b) If an employee fails to comply with this Program, the matter will be referred to the AML/CTF CO immediately. The AML/CTF CO may then take any of the following actions:
 - (i) undertake an internal spot check on the employee's performance to check compliance with iTeller's policies and procedures;
 - (ii) implement a higher level of supervision of the employee;
 - (iii) provide a warning to the employee for non-compliance with procedures and breach of the Program; or
 - (iv) if breaches are repeated without reasonable excuse, consider transferring or dismissing the employee in consultation with the Director.

18. RISK AWARENESS TRAINING PROGRAM

- 18.1 iTeller implements a Risk Awareness Training Program ("**RATP**") designed to ensure each employee receives appropriate ongoing training on the ML/TF risk that iTeller may face.
- 18.2 The RATP is designed to enable employees to understand:
 - (a) iTeller'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 iTeller might face and the potential consequences of such risk; and
 - (d) those processes and procedures provided for by this Program which are relevant to the work carried out by the employee.
- 18.3 All new employees are required to undergo the RATP as part of their induction process. All employees that are in positions identified as having ML/TF risk are required to undertake training on an annual basis, or whenever the AML/CTF CO considers necessary, for example when a new product or delivery channel is introduced.
- 18.4 The AML/CTF CO is responsible for maintaining the training register for both the induction training and any ongoing training conducted for each employee.

- 18.5 **Induction Training** – All employees are required to complete AUSTRAC's [Induction Program for new Reporting Entities](#) upon commencement of their employment with iTeller. Employees of iTeller are required to obtain a pass mark of over 85%.
- 18.6 **Ongoing Compliance Training** – The AML/CTF CO may decide when compliance training by an external compliance consultant is necessary. The AML/CTF CO must, upon completion of the training, make the training materials available to all employees. 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 CO.
- 18.7 **In-house AML/CTF Seminars** – The AML/CTF CO may decide when to organise the in-house AML/CTF seminars. The AML/CTF CO will organise such seminars on a regular basis so that employees who come back to work from leave will have the opportunity to refresh their knowledge, and so employees can remain up to date with the latest risk trends and best practices in the industry.
- 18.8 **Non-attendance of Training Sessions** – Non-attendance at any training sessions, without reasonable excuse, will be reported to the Director and the AML/CTF CO will take any disciplinary action they consider necessary.
- 18.9 **Compliance Policies** – all new employees will receive a copy of this Program and all compliance policies of iTeller within a reasonable time of commencing employment. All employees are expected to review these compliance policies on a regular basis and will be required to complete a declaration stating that they have read the compliance policies.
- 18.10 **Document Retention Policy** – the AML/CTF CO must encourage all employees to read and understand the Document Retention Policy. Employees who fail, without reasonable excuse, to read the Document Retention Policy will be reported to the Director who will take disciplinary action as they consider necessary.

19. OUTSOURCING

OUTSOURCING	
Outsourcing – due diligence requirements:	<p>Prior to iTeller outsourcing any of its AML/CTF obligations, it will:</p> <ul style="list-style-type: none"> (a) have an agreement in place with the party to whom the activities are outsourced (“Third Party Providers”); (b) where relevant, require the Third-Party Providers to whom the activities are outsourced to implement the policies and procedures outlined in this Program;

	<ul style="list-style-type: none"> (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 will not increase the ML/TF risk iTeller faces; (e) conduct due diligence on the Third-Party Providers to ensure that outsourcing activities to these parties will not increase the ML/TF risk iTeller faces; (f) ensure that all Third-Party Providers understand: <ul style="list-style-type: none"> (i) iTeller'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 iTeller 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.
Additional due diligence requirements where outsourcing customer identification functions:	<p>In addition to the due diligence requirements above, iTeller will:</p> <ul style="list-style-type: none"> (a) conduct due diligence on the Third-Party Providers to ensure they hold the appropriate licences and/or registrations with ASIC, AUSTRAC or any other relevant regulator; (b) ensure Third Party Providers have an AML/CTF Policy in place which complies with the Act and Rules; and (c) ensure the agreement in place between iTeller and Third-Party Providers permits access to the KYC records of iTeller's clients. <p>When assessing the ML/TF risk associated with a Third-Party Provider undertaking customer identification procedures on its behalf having regard to the following factors:</p> <ul style="list-style-type: none"> (a) the existence and quality of Third-Party Providers' AML/CTF Policy; (b) the resources of Third-Party Providers, including the number of staff and access to technological resources; (c) the outcome of due diligence undertaken in respect of Third-Party Providers; and (d) quotes received and references from former and current partners of Third-Party Providers.
Reviews:	The AML/CTF CO will undertake quarterly reviews of all Third-Party Providers to assess whether the Third-Party Provider:

	<ul style="list-style-type: none"> (a) has performed their functions within the scope of the agreement with iTeller; (b) maintains appropriate resources, licences and registrations; (c) has met their AML/CTF obligations under the AML/CTF Act and Rules; and (d) has caused an increase in the ML/TF risk iTeller faces.
--	--

19.1 iTeller maintains a separate Third-Party Providers register, detailing:

THIRD PARTY PROVIDER REGISTER					
Service Provider	Service Outsourced	Date of Appointment	Frequency of Review	Date of Review	Outcome of Review

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

20.1 iTeller does not provide designated services through permanent establishments in foreign countries.

20.2 If at any time iTeller begins to provide designated services at or through permanent establishments in foreign countries, the AML/CTF CO will review this Program in its entirety, prepare a risk assessment and propose any necessary changes to the Director for approval. The Board will, in consultation with senior management and any external compliance consultant, review and consider the proposed changes taking into account of any ML/TF risks imposed by provision of designated services through a permanent establishment in that particular jurisdiction.

21. RELIANCE ON THIRD PARTY CUSTOMER IDENTIFICATION PROCEDURES

21.1 iTeller will ensure that any third party it engages with for customer identification procedures is:

- (a) another reporting entity regulated by AUSTRAC; or

(b) regulated foreign equivalents which are subject to equivalent AML/CTF obligations for customer due diligence and record keeping;

(c) A proper agreement between iTeller and any third party will be in place for the same.

21.2 **Ongoing arrangement** – iTeller has entered into a written arrangement or arrangement with the third party provider. iTeller has conducted due diligence on the third party provider to ensure that the third party provider has appropriate AML/CTF systems and controls to meet each of the requirements prescribed under Chapter 7 of the AML/CTF Rules prior to entering into the customer due diligence (“**CDD**”) arrangement.

21.3 iTeller must record its CDD arrangements in writing and these arrangements must be approved by the Director.

The CDD arrangement must include:

(a) an outline of the responsibilities of each of the parties to the arrangement;

(b) provisions to enable the relying reporting entity to obtain all required KYC information relating to the identity and verification details on request and without delay including:

(i) the customer;

(ii) the Beneficial Owner of the customer; and

(iii) a person acting on behalf of the customer.

21.4 iTeller must complete an assessment of its CDD arrangements every two (2) years, or as required.

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

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

(a) the procedures undertaken; and

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

- 22.2 A copy of these records will be retained for at least seven (7) years after iTeller has ceased to provide designated services to the customer.
- 22.3 Records to be retained under this section (whether in electronic or hard copy form) must be easily identifiable, easily located and easily retrievable, in order to:
- (a) provide the record to an AUSTRAC authorised officer within a reasonable period; and
 - (b) demonstrate to the AUSTRAC authorised officer that iTeller has complied with the obligations under subsection 112(2) of the AML/CTF Act.
- 22.4 Records retained under this section are limited to employees of iTeller on a need-to-know basis. Where an employee leaves iTeller, access to the records retained under this section is revoked.
- 22.5 A copy of any other record made by iTeller 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.
- 22.6 Where possible, iTeller ensures all records are held on a server located in Australia and not in a foreign jurisdiction.
- 22.7 Details of record keeping and handling are set out in iTeller's Document Retention Policy.

23. TRANSACTION MONITORING

- 23.1 iTeller's transaction monitoring program consists of three steps:
- (a) Monitoring all customer transactions in accordance with iTeller's policies, systems and procedures;
 - (b) Identifying all suspicious transactions; and
 - (c) Taking the appropriate action.
- 23.2 The AML/CTF CO will review the transaction monitoring system in consultation with the Director and iTeller's external compliance consultant.
- 23.3 The AML/CTF CO has the primary responsibility for transaction monitoring for iTeller. All transaction reports will be reviewed by the Director on a monthly basis.

23.4 All of iTeller's employees will receive training in transaction monitoring as part of the RATP.

23.5 As required by the AML/CTF Act, iTeller will provide reports to AUSTRAC in an approved form that contains the required information. The table below provides a summary of iTeller's reporting obligations:

SUMMARY OF REPORTING OBLIGATIONS				
Compliance Obligations	Compliance Requirements	Compliance Actions	Responsible Person	Frequency
Annual AUSTRAC Compliance Report	Submit the annual compliance report to AUSTRAC by the deadline.	Ensure that AUSTRAC Compliance Report is completed in line with AUSTRAC regulations and are submitted accordingly – usually by 31 March each year.	AML/CTF CO	Annually
Changes to iTeller's AUSTRAC enrolment	Notify AUSTRAC of any change in business details.	Ensure that changes to iTeller's business details are reported to AUSTRAC within fourteen (14) days.	AML/CTF CO	As required – within fourteen (14) days.
Suspicious Matter Reporting (SMR)	Implement and monitor SMR procedures.	Ensure all SMRs are reported to AUSTRAC within the required timeframe. An SMR must be submitted within three (3) business days of forming the suspicion. If the suspicion relates to the financing of terrorism, the SMR must be submitted within twenty-four (24) hours of forming the suspicion.	AML/CTF CO	As required – within three (3) business days or twenty-four (24) hours.
Threshold Transaction Reporting (TTR)	Implement and monitor TTR procedures.	Ensure all TTRs are reported to AUSTRAC within ten (10) business days of the threshold transaction taking place.	AML/CTF CO	As required – within ten (10) business days.

International Fund Transfer Instructions (IFTI)	Implement and monitor IFTI procedures.	Ensure all IFTIs are reported to AUSTRAC within ten (10) business days of sending or receiving the instruction.	AML/CTF CO	As required – within ten (10) business days.
--	--	---	------------	--

23.6 iTeller will use the following methods for electronic reporting via AUSTRAC Online at <https://online.austrac.gov.au/ao/login.seam>:

- (a) **Data entry:** The required report information can be manually entered into AUSTRAC Online account at <https://online.austrac.gov.au/ao/login.seam>. All three types of report (TTRs, IFTIs and SMRs) may be reported via this method; and
- (b) **Extraction:** Through iTeller's AUSTRAC Online account or upon request, AUSTRAC can supply the file format specifications and/or XML schemas that will enable a regulated entity to write an extraction program. This program will extract the relevant information from an existing database and collate it in a single file, which is submitted or transmitted to AUSTRAC Online account. This option is available for TTRs, IFTIs and SMRs.


24. SUSPICIOUS MATTER REPORTING

24.1 iTeller adopts a 'Red Flag' policy which requires employees to complete a Red Flag Indicator Sheet (please refer to

24.2 B of this Program) for each new client and as a procedure to conduct ongoing transaction monitoring. iTeller's policies and procedures for suspicious matter reporting are set out in the table contained in Section 24.1.

SUSPICIOUS MATTER REPORTING	
Responsible Person	AML/CTF CO
Supervision	The Director of iTeller has overall responsibility and oversight of iTeller's transaction reporting and monitoring program. The Director conducts monthly review of all SMRs submitted during the previous month in order to identify systemic issues.
1. What are the Suspicious Matter Reporting obligations?	
General Rules	iTeller must submit a SMR to AUSTRAC if:

	<p>(a) iTeller commences to provide, or proposes to provide, a designated service to a person; or</p> <p>(b) a person requests iTeller provides a designated service (of a kind ordinarily provided by us), or</p> <p>(c) a person makes an enquiry to iTeller as to whether it would be willing provide a designated service (of a kind ordinarily provided by iTeller);</p> <p>and iTeller forms a suspicious <u>on reasonable grounds</u> that:</p> <p>(a) a person (or their agent) is not the person they claim to be, or</p> <p>(b) information we have may be:</p> <p>(i) relevant to the investigation or prosecution of a person for:</p> <p>A. an offence against a law of the Commonwealth, a State or Territory;</p> <p>B. an evasion, or an attempted evasion, of a taxation law (as defined in the <i>Taxation Administration Act 1953</i> (Cth)) or a law of a State or Territory that deals with taxation; or</p> <p>C. a ML/TF offence;</p> <p>(ii) of assistance in the enforcement of laws relating to proceeds of crime; or</p> <p>(c) providing a designated service may be:</p> <p>(i) preparatory to committing an offence related to ML or TF, or</p> <p>(ii) relevant to the investigation or prosecution of a person for an offence related to ML or TF.</p>
Who is covered by the general rules?	Existing, new or potential customers, or an agent of an existing, new or potential customer.
When to report to AUSTRAC?	<p>iTeller must submit a report to AUSTRAC if, after conducting enhanced due diligence checks, the AML/CTF CO has formed a suspicion that a criminal offence has occurred, or they have identified at least one (1) red flag indicator, regardless of whether iTeller's client is the victim or the offender.</p> <p>iTeller's employees and AML/CTF CO are NOT necessarily expected to know or to establish:</p>

	<p>(a) the exact nature of any criminal offence the customer may be involved in, or</p> <p>(b) particular funds or property have been acquired through illicit or criminal means.</p>
2. Identification of Suspicious Activities and Suspicious Customer Behaviour	
Red Flag Policy	iTeller adopts a 'Red Flag' policy which requires employees to complete the Red Flag Indicators Sheet and put a red flag when a red flag indicator exists.
Red Flag Indicators	<p>iTeller develops a list of Red Flag Indicators Sheet (Annexure B). This sheet is updated on an ongoing basis.</p> <p>iTeller requires a copy of Annexure B to be completed:</p> <p>(a) for each new client – before the provision of a designated service; and</p> <p>(b) for existing clients – on a half yearly basis or whenever the AML/CTF CO considers necessary.</p>
What happens when a Red Flag is identified?	<p>Reporting Line:</p>  <pre> graph LR Employee[Employee] --> Supervisor[Immediate Supervisor] Supervisor --> AMLCTF[AML/CTF CO] AMLCTF --> AUSTRAC[AUSTRAC] </pre>
	Existence of 1 Red Flag:
	<p>The employee responsible should:</p> <p>(a) conduct the enhanced due diligence procedures set out in this Program and refer the matter to the immediate attention of their supervisor – the employee must not discuss the matter with anyone else except his/her immediate supervisor or the AML/CTF CO;</p> <p>(b) the supervisor will report to the AML/CTF CO once the results of enhanced due diligence are received; and</p> <p>(c) the AML/CTF CO then submits an SMR to AUSTRAC.</p>
Suspicion in relation to the identity of a customer	<p>If the AML/CTF CO is notified of a suspicion relating to the identity of the customer, the AML/CTF CO must, within fourteen (14) days commencing after the day on which the AML/CTF CO was notified of the suspicion, do one of the following for the purpose of enabling iTeller to be reasonably satisfied that the customer is the person that he or she claims to be:</p> <p>(a) review all KYC information in respect of the customer;</p>

	<p>(b) re-verify, from a reliable and independent source, any KYC Information that has been obtained in respect of the customer; or</p> <p>(c) verify, from a reliable and independent source, any previously unverified KYC Information that has been obtained in respect of the customer.</p> <p>If:</p> <p>(a) after reviewing the enhanced due diligence information from a customer in accordance with this Program, the AML/CTF CO is still not satisfied that the customer is who they claim to be; or</p> <p>(b) the AML/CTF CO is unable to collect any additional information from the customer,</p> <p>then the AML/CTF CO <u>must</u> make a SMR to AUSTRAC.</p>
Suspicion in relation to an existing customer	<p>If the AML/CTF CO forms a reasonable suspicion in respect of an existing customer of iTeller, the AML/CTF CO must, within fourteen (14) days commencing after the day on which the AML/CTF CO formed the suspicion, carry out the applicable customer identification procedures in Part B.</p> <p>If the applicable customer identification procedures in Part B cannot be performed because iTeller:</p> <p>(a) has doubts about the veracity or adequacy of previously obtained documents or information obtained when conducting the applicable customer identification procedures or when relying on a reliable third party; or</p> <p>(b) suspects on reasonable grounds that the customer is not the person that the customer claims to be;</p> <p>the AML/CTF CO must submit a SMR.</p>
3. Discussion or Communication about the SMR	
Immediate Supervisor or the AML/CTF CO	<p>iTeller's employees or representatives must ONLY discuss the matter with their immediate supervisor, or the AML/CTF CO when their immediate supervisor is not available, unless as otherwise authorised by the AML/CTF CO.</p> <p>After the employee forms an initial suspicion about a customer, he/she should use discretion when making further enquiries about the customer, to minimise the risk of the customer realising an SMR has been submitted about them.</p>
AUSTRAC CEO	<p>Once iTeller has fulfilled the obligation to provide the relevant information about a suspicious matter to the AUSTRAC CEO, iTeller's employees and representatives must not disclose to anyone other than the AUSTRAC CEO or a member of the staff of AUSTRAC that the information has been communicated to the AUSTRAC CEO.</p>

4. Submitting an SMR

Assessment of the situation and SMR

If iTeller's AML/CTF CO receives a notification in relation to a suspicious matter, the AML/CTF CO must:

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

If the AML/CTF CO determines that a SMR must be lodged in relation to a customer, iTeller will:

- (a) keep all records of the results of any enhanced customer due diligence conducted; and
- (b) report the suspicion to the AUSTRAC CEO through submitting an SMR in an approved form in accordance with the requirements of the AML/CTF Act and Rules:
 - (i) within twenty-four (24) hours after the time when the AML/CTF CO 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 CO forms the relevant suspicion;
- (c) consult with AUSTRAC and other relevant enforcement agencies to determine how best to deal with the customer, if required; and
- (d) continue to transact with the customer on the usual basis until further advised by AUSTRAC and other relevant enforcement agencies.

When submitting an SMR, the AML/CTF Act will protect iTeller from civil or criminal liability when information is provided in an SMR in compliance with iTeller's obligations under the AML/CTF Act.

5. Can iTeller continue providing services if it has formed a suspicion about the customer?

The AML/CTF Act does not direct reporting entities to stop providing designated services to, or terminate a business relationship with, a customer, even if iTeller has formed a suspicion about that particular customer. iTeller must determine whether to terminate the relationship with the customer based on its own risk-assessment, procedures and controls.

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

<p>(a) iTeller must not disclose to the customer that it has formed a suspicion and/or communicated the suspicion to AUSTRAC – this is referred to as “tipping off” the customer; and</p> <p>(b) iTeller must continue to comply with the AML/CTF Act in all future dealings with that customer, which may include submitting additional SMRs.</p>	
<p>Tipping Off Provisions</p>	<p>iTeller must NOT disclose to any person (other than AUSTRAC) that it formed a suspicion about a customer or that it submitted an SMR to AUSTRAC. Doing so would constitute 'tipping off', which is an offence prohibited by section 123 of AML/CTF Act.</p> <p>Reporting Entities that submit SMRs also have additional obligations under the AML/CTF Act not to disclose any:</p> <p>(a) information that might reasonably lead a person to conclude that they formed a suspicion about a customer or that we communicated that suspicion to AUSTRAC; and</p> <p>(b) requests from AUSTRAC for further information about an SMR report.</p> <p>AUSTRAC considers that simply asking a customer for additional information (for example, about their identity or the source or destination of their funds) would not constitute an unlawful disclosure of information or an offence under the tipping off provisions of the AML/CTF Act.</p> <p>There are exemptions under the AML/CTF Act for the tipping off provisions which includes when iTeller discloses information about a SMR to:</p> <p>(a) a legal practitioner to obtain legal advice;</p> <p>(b) an auditor engaged to conduct an audit or review of the AML/CTF Program; or</p> <p>(c) foreign members of the same corporate or DBG with which iTeller has shared customers but only if the foreign members are regulated by laws of a foreign country that give effect to some or all of the Financial Action Task Force (“FATF”) recommendations.</p>
<p>6. Other Resources</p>	
<ul style="list-style-type: none"> • AUSTRAC Website: http://www.austrac.gov.au/suspicious-matter-reports-smrs • The Australian Typologies and Case Studies Reports, available at http://www.austrac.gov.au/typologies.html • Financial Action Task Force and its guidance, available at: http://www.fatf-gafi.org 	

25. TRANSACTION REPORTING - THRESHOLD TRANSACTION REPORTS

25.1 Definitions:

- (a) **Physical Currency** – the coin or printed money of Australia or another country which is designated as legal tender;
- (b) **Digital Currency** –
 - (i) a digital representation of value that:
 - A. functions as a medium of exchange, a store of economic value, or a unit of account; and
 - B. is not issued by or under the authority of a government body; and
 - C. is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and
 - D. is generally available to members of the public without any restriction on its use as consideration; or
 - (ii) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;

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

25.2 Under the AML/CTF Act, if iTeller provides a designated service to a customer which involves the transfer of physical currency of AUD10,000 or more (or the foreign currency equivalent), iTeller must submit a threshold transaction report (“**TTR**”) to AUSTRAC.

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

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

25.5 The TTR must be in the approved form and sent in accordance with the requirements of the Rules. Please see details of the requirement in the table below.

WHAT SHOULD BE INCLUDED IN A TTR?	
General Requirements:	<ul style="list-style-type: none"> (a) The date of the threshold transaction; (b) A description of the designated service provided or commenced to be provided by iTeller to the customer which involves the threshold transaction; (c) The total amount of funds provided to or received from the customer; and (d) Details of the threshold transaction, including whether it involved physical currency or digital currency.
Additional Requirement - if the customer is an individual	<ul style="list-style-type: none"> (a) the customer's full name; (b) any other name used by the customer, if known; (c) any business name(s) under which the customer operates, if known; (d) the customer's date of birth; (e) the customer's full address (not being a post office box address); (f) the postal address of the customer if different from their full address; (g) the customer's telephone number, if known; (h) the ABN of the customer, if known; and (i) if the person conducting the threshold transaction is not the customer, the details for the person specified in the above (a) to (c).
Additional Requirement – if the customer is a business	<ul style="list-style-type: none"> (a) The name of the customer and any business name(s) under which the customer operates; (b) A description of the legal form of the customer and any business structure it is a part of, if known; (c) The full address of the customer's principal place of business; (d) The postal address of the customer if different from the full address; (e) The ACN, ARBN and/or ABN of the customer, if known; (f) The customer's telephone number, if known; and

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

26. TRANSACTION REPORTING - INTERNATIONAL FUNDS TRANSFER INSTRUCTION REPORTS – INTERNATIONAL FUNDS TRANSFER INSTRUCTION UNDER A DESIGNATED REMITTANCE ARRANGEMENT

26.1 Under the Act, if iTeller sends or receives an instruction:

- (a) accepted at or through a permanent establishment of a 'non-financier' in Australia, where the person who receives the instruction is to make, or arranges to make, money or property available to the ultimate transferee at or through a permanent establishment of a person in a foreign country; or
- (b) accepted at or through a permanent establishment of a person in a foreign country where a 'non-financier' is to make, or arranges to make, money or property available to the ultimate transferee through a permanent establishment of the non-financier in Australia;

iTeller must submit an international funds transfer instruction under a designated remittance arrangement (“**IFTI-DRA**”) report to AUSTRAC.

26.2 The term ‘non-financier’ is defined in section 5 of the Act as a person who is not an ADI, a bank, a building society, a credit union or a person specified in the AML/CTF Rules.

26.3 The IFTI report must be in the approved form and sent in accordance with the requirements of the AML Rules. Section 23.6 sets out three (3) different ways of preparing IFTI reports. Depending on the size of iTeller’s business, iTeller may use different report formats as determined by the AML/CTF CO.

26.4 The table below outlines the details of the requirement:

IFTI - DRA	
Rules	Under the Act, if iTeller sends or receives an instruction to or from a foreign country for a transfer of money or property under a remittance arrangement, iTeller must submit an IFTI report to AUSTRAC. The reporting obligations for IFTIs are set out in sections 45 and 46 of the Act.

IFTI-DRA	<p>IFTI-DRA's are set out in item 3 and item 4 of section 46 of the Act.</p> <p>iTeller is a designated remittance services provider and will be required to lodge IFTI-DRA under the Act.</p> <p>There are two types of IFTI-DRA's:</p> <p>(a) <u>IFTI-DRA (outgoing)</u></p> <p>These are instructions transmitted out of Australia.</p> <p>(b) <u>IFTI-DRA (incoming)</u></p> <p>These are instructions transmitted into Australia.</p>
iTeller's Process	<p>(a) When an employee of iTeller receives an international funds transfer instruction from a customer, they must refer this instruction immediately to their supervisor;</p> <p>(b) The supervisor will report to the AML/CTF CO on a daily basis on all international funds transfer instructions; and</p> <p>(c) The AML/CTF CO must submit an IFTI-DRA in an approved form to the AUSTRAC CEO within 10 business days of the transaction taking place.</p>
Information required for an IFTI-DRA (Outgoing)	<p>(a) iTeller must complete all required elements of the relevant form (for single transaction report) or the spreadsheet (for bulk transaction reports) via AUSTRAC Online.</p> <p>(b) Where the transferor is an individual: the information required in an IFTI-DRA is included in section 17.2(1) of the AML/CTF Rules.</p> <p>(c) Where the transferor is a non-individual: the information required in an IFTI-DRA is included in section 17.2(2) of the AML/CTF Rules.</p> <p>Other information required for both individual and non-individuals: is included in section 17.2(3)-(13) of the AML/CTF Rules.</p>

Information required for an IFTI-DRA (Incoming)	<ul style="list-style-type: none"> (a) iTeller must complete all required elements of the relevant form (for single transaction report) or the spreadsheet (for bulk transaction reports) via AUSTRAC Online. (b) Where the transferor is an individual: the information required in an IFTI-DRA is included in section 17.3(1) of the AML/CTF Rules. (c) Where the transferor is a non-individual: the information required in an IFTI-DRA is included in section 17.3(2) of the AML/CTF Rules. (d) Foreign entity that accepts instructions from the transferor – if the foreign entity is an individual: is included in section 17.3(3)(a) of the AML/CTF Rules. (e) Foreign entity that accepts instructions from the transferor – if the foreign entity is a non- individual: is included in section 17.3(3)(b) of the AML/CTF Rules. (f) Other information required for both individual and non-individuals: is included in section 17.3(4)-(14) of the AML/CTF Rules.
<u>Copies of Funds Transfer Messages</u>	<p>A copy of the funds transfer message transmitted into Australia may be given as a report of an IFTI-DRA in accordance with the applicable approved form. The report:</p> <ul style="list-style-type: none"> (a) must contain the information required under subsection 16.3 of the Rules; and (b) may contain information giving effect to the international funds transfer as required: <ul style="list-style-type: none"> (i) by message format standards; (ii) by message usage guidelines; or (iii) to complete the transfer including, but not limited to: <ul style="list-style-type: none"> A. who initiated the transfer on behalf of the payer; B. additional contact information for the payer and payee; (c) remittance information about the invoice or garnishment administration.
IFTI Reports – information on the	<p>A report under subsection 45(2) of the Act must contain the following details about the person completing the report:</p>

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

27. AML/CTF COMPLIANCE REPORTS

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

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

28. CHANGES TO ITELLER'S AUSTRAC ENROLMENT/REGISTRATION DETAILS

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

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

- (a) changes to enrolment details on AUSTRAC Business Profile Form which can be obtained from iTeller's AUSTRAC Online Account;
- (b) changes in the number of key personnel at iTeller and a declaration that police and bankruptcy checks have been obtained;
- (c) whether any key personnel of iTeller have been criminally charged; and
- (d) whether iTeller is the subject of civil or criminal proceedings or enforcement action.

28.3 Notification of a change of iTeller's enrolment details may be made by an agent of iTeller where:

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

- (b) that agreement or written authority authorises the agent to notify, on behalf of iTeller, a change in the enrolment details of iTeller on the Reporting Entities Roll; and
- (c) the notification of a change in iTeller's enrolment details includes a declaration by the agent that the information is true, accurate and complete.

29. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

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

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

29.3 In these circumstances, the AML/CTF CO will determine whether the matter should be reported to AUSTRAC as a suspicious matter (please refer to section 24 of this Program).

30. ONGOING CUSTOMER DUE DILIGENCE

30.1 iTeller, as a Digital Currency Exchange Provider, will monitor its own customers in accordance with this Section for the purpose of identifying, mitigating and managing the ML/TF risk that the provision of a designated service at or through a permanent establishment in Australia may involve.

30.2 iTeller will comply with the ongoing customer due diligence procedures outlined in the table below.

ONGOING CUSTOMER DUE DILIGENCE MANAGEMENT SYSTEM			
Types of customers that the Reporting Entity <u>will</u> provide services to:	(a) Individuals;	Types of customers that the Reporting Entity <u>will not</u> provide services to:	(a) Agents (b) Companies; (c) Trusts; (d) Trustees and beneficiaries; (e) Partnerships; (f) Associations; (g) Registered cooperatives; (h) Government bodies; and (i) Any other entity, structure, organisation which is not an individual.
Review of Customer types:	The Reporting Entity's AML/CTF CO is responsible for reviewing and updating the customer types that we provide services to on an ongoing basis.		
The Reporting Entity will monitor customers by implementing systems to: (a) collect further KYC Information for ongoing customer due diligence processes; (b) update and verify KYC Information for ongoing customer due diligence purposes; (c) monitor the transactions of customers; and (d) conduct enhanced customer due diligence in respect of high risk customers and customers about whom a suspicion has been formed.			
Grouping of customers:	As part of implementing systems for ongoing customer due diligence purposes, the Reporting Entity will group customers according to their level of risk, which has been assessed as part of the risk assessment procedures outlined in this Program. The risk grouping will determine:		

	<p>(a) what further KYC Information needs to be collected for ongoing customer due diligence purposes in respect of a particular customer;</p> <p>(b) what level of transaction monitoring needs to be conducted in relation to a customer; and</p> <p>(c) whether the enhanced customer due diligence program needs to be applied.</p> <p>The AML/CTF CO is responsible for the grouping of customers in accordance with the risk assessment procedures outlined in this Program. The AML/CTF CO will review the grouping of customers on a monthly basis, and the Board will conduct spot check on the grouping of customers on a half-yearly basis.</p>
ADDITIONAL KYC INFORMATION	
Risk Assessment for New Activities and Technologies:	In undertaking the risk assessment for new activities and technologies, the AML/CTF CO will determine whether any additional KYC Information or Beneficial Owner information should be collected from relevant customers either before any designated services are provided to the customer or during the course of iTeller's relationship with the customer. These requirements will be incorporated into the relevant customer identification procedures.
Assessment on the level of ML/TF risk involved for different type of customers:	<p>Based on the assessed level of the ML/TF risk involved in the provision of designated services provided by the Reporting Entity as at the date of this Program, iTeller has determined that:</p> <p>(i) Low Risk Customers - no additional KYC Information needs to be collected;</p> <p>(ii) Medium Risk Customers - the AML/CTF CO will determine what additional KYC Information or Beneficial Owner information will be collected as ongoing customer due diligence.</p> <p>(iii) High Risk Customers - the AML/CTF CO will determine what additional KYC Information or Beneficial Owner information will be collected as ongoing customer due diligence.</p> <p>In relation to collection of additional KYC information, please refer to the relevant customer type under Part B of the Program.</p>
New Customers:	In respect of a new customer, the additional KYC Information will be collected at the same time as and in the same manner as the KYC Information is required to be collected under Part B. Failure to provide

	additional KYC Information will be treated in the same way as the failure to provide any other KYC Information collected under Part B.
Existing Customers	<p>In respect of an existing customer or Beneficial Owner, iTeller updates and re-verifies KYC Information by requesting additional KYC Information where the AML/CTF CO considers the KYC Information is no longer up-to-date, incomplete or unreliable or in accordance with the below timeframes. The Reporting Entity may also request additional KYC information where the scope of the services provided to an existing customer changes.</p> <ul style="list-style-type: none"> (a) High-risk customers – annually (b) Medium risk customers – every two (2) to three (3) years (c) Low risk customers – every three (3) to five (5) years
When to update and re-verify KYC Information:	<p>iTeller updates and re-verifies KYC Information in respect of a customer where:</p> <ul style="list-style-type: none"> (a) the customer engages in a significant transaction or series of transactions with one or more reporting entities, where a significant transaction occurs if a transaction, or series of transactions conducted within any calendar month exceeds Ten Thousand Dollars (\$10,000.00) of digital currency or physical currency in value; or (b) a significant change occurs: <ul style="list-style-type: none"> (i) in the way the customer conducts transactions; (ii) in the nature of the customer's business or business relationship; (iii) in the customer's control structure; (iv) in the customer's beneficial ownership; or (v) in the number of transactions carried out by a customer increases by 100% within a five (5) calendar day period. <p>Where one of the above circumstances arises in respect of a customer and the applicable customer identification procedure has not previously been carried out in respect of a customer (i.e. the customer is a</p>

	<p>pre-commencement customer), the Reporting Entity will carry out the applicable customer identification procedure in accordance with Part B and collect the relevant additional KYC Information.</p> <p>Where a change in customer information relates to in the case of:</p> <ul style="list-style-type: none"> (a) individual customers, their: <ul style="list-style-type: none"> (i) name; or (ii) residential address; (b) a company: <ul style="list-style-type: none"> (i) the company's name; or (ii) the company's registration number; (c) a trust: <ul style="list-style-type: none"> (i) the trustee; or (ii) the name of the trust; and (d) in the case of a partnership, the identity of a partner; <p>iTeller seeks to verify the updated KYC Information using reliable and independent documentation in accordance with Part B of this Program.</p>
TRANSACTION MONITORING PROGRAM	
Responsible Persons:	<p>The Director and the AML/CTF CO have overall responsibility and oversight of the Reporting Entity's transaction-monitoring program.</p> <p>The Reporting Entity conducts transaction monitoring on a monthly basis.</p>
Identification of Risk Factors:	<p>The AML/CTF CO must identify ML/TF risk factors relevant to customers of particular services and products provided by us. Such risk factors include the:</p> <ul style="list-style-type: none"> (a) value of the transaction exceeds Ten Thousand Dollars (\$10,000.00) of digital currency or physical currency in value;

	<ul style="list-style-type: none"> (b) volume of transactions conducted by a customer within a five (5) calendar day period has increased by more than one hundred per cent (100%); (c) transaction involves foreign countries, customers or third parties against whom sanctions have been imposed or have been included on the lists maintained by the Department of Foreign Affairs and Trade under the <i>Charter of United Nations (Terrorism and Dealings with Assets) Regulations 2002</i> (Cth); or (d) transaction involves a customer or third party who is a PEP.
Steps to Take After One or More Risk Factors Have Been Identified:	<ul style="list-style-type: none"> (a) An employee must immediately inform the AML/CTF CO when any ML or TF risk factor(s) are identified in relation to a customer or a customer's representative; (b) The AML/CTF CO will then liaise with the [Board/Director] in relation to any further action by the Reporting Entity including, but not limited to the items listed in the "Further Actions to take" section below. (c) Where an employee identifies a customer or third party of a kind specified in item (c) and (d) in "Identification of Risk factors" section above, the AML/CTF CO 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.
Further Actions to Take:	<p>If it is determined, as a result of transaction monitoring, that:</p> <ul style="list-style-type: none"> (a) a customer should be placed in a higher risk grouping, the Reporting Entity will collect additional KYC Information if required with Section 30 of this Program; (b) KYC Information needs to be updated or verified in respect of a customer, iTeller will update or verify the required information with Section 30 of this Program; (c) a customer is a high-risk customer, iTeller will apply the enhanced customer due diligence program set out below; or (d) a suspicious matter report needs to be lodged in respect of a customer, iTeller will follow the procedure outlined in Section 24 of this Program.

Training on Identification of Risk Factors:	In addition to the Risk Awareness Training referred to in this Program, the AML/CTF CO will ensure that all employees of iTeller who have direct contact with customers or their representatives, receive regular training in the identification of ML/TF risk factors.
Review and Update of iTeller's Transaction Monitoring Program:	<p>The AML/CTF CO, in consultation with the Director, must regularly assess iTeller's transaction monitoring program and should take steps to have this modified appropriately:</p> <ul style="list-style-type: none"> (a) where there has been a significant change in the ML or TF risk relating to designated services provided by iTeller; (b) prior to iTeller introducing a new designated service to the market; (c) prior to iTeller adopting a new method of delivering a designated service; (d) prior to iTeller adopting a new technology or developing technology used for the provision of an existing or new designated service; and (e) where the AML/CTF CO identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of iTeller's customers.
ENHANCED CUSTOMER DUE DILIGENCE PROGRAM	
Responsible Persons:	The AML/CTF CO has overall responsibility and oversight of iTeller's enhanced customer due diligence program.
Factors for Conducting Enhanced Customer Due Diligence Program:	<p>The ML/TF risk associated with a particular designated service, customer, delivery method or jurisdiction is high, including but not limited to when:</p> <ul style="list-style-type: none"> (a) the customer: <ul style="list-style-type: none"> (i) is engaged in business which involves a significant number of cash transactions or amounts of cash; or (ii) uses a complex business ownership structure for no apparent commercial or other legitimate reason, especially if the Beneficial Owners of the legal entity cannot be determined; or (iii) is based in, or conducts business through or in, a high-risk jurisdiction; or

	<ul style="list-style-type: none"> (iv) cannot provide information to verify the source of funds; or (v) requests an undue level of secrecy in relation to a designated service; or (vi) is a PEP; or (b) a designated service is being provided to a customer who is or who has a Beneficial Owner who is, a foreign politically exposed person; or (c) suspicion has arisen for the purposes of section 41 of the AML/CTF Act (refer to Section 24 of this Program); or (d) iTeller is entering into or proposing to enter into a transaction and a party to the transaction is physically present, or is a company incorporated in, a prescribed foreign country.
Steps to Take After One or More Factors Above Have Been Identified:	<p>Where one or more of the factors above arises, the AML/CTF CO will arrange for one or more of the following due diligence procedures to occur:</p> <ul style="list-style-type: none"> (a) seek further information from the customer or from third party sources in order to: <ul style="list-style-type: none"> (i) clarify or update the customer's KYC Information or Beneficial Owner information already collected from the customer, in accordance with 'Additional KYC Information' above under this Section; and (iii) clarify the nature of the customer's ongoing business with iTeller. (b) conduct more detailed analysis in respect of the customer's KYC Information and Beneficial Owner information taking reasonable measures to identify: <ul style="list-style-type: none"> (i) the source of the customer's and each Beneficial Owner's wealth; and (ii) the source of the customer's and each Beneficial Owner's funds; (c) verify or re-verify KYC Information or Beneficial Owner information in accordance with the customer identification program outlined in Part B of this Program; (d) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future, including but not limited to: <ul style="list-style-type: none"> A. the purpose, reasons for, or nature of specific transactions;

	<p>B. the expected nature and level of transaction behaviour, including future transactions;</p> <p>(e) consider whether a Suspicious Matter Report ought to be lodged in accordance with section 41 of the AML/CTF Act (refer to Section 24 of this Program); and</p> <p>(f) consider whether a transaction or particular transactions should be processed.</p> <p>Where necessary the AML/CTF CO may also:</p> <p>(a) obtain any further KYC Information or Beneficial Owner information in accordance with the 'Additional KYC Information' requirements above in this table, including where appropriate, taking reasonable measures to identify:</p> <ul style="list-style-type: none"> (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; and <p>(b) seek Director approval for:</p> <ul style="list-style-type: none"> (i) continuing a business relationship with a customer; and (ii) whether a designated service should continue to be provided to the customer.
<p>Steps to Take where a customer or a Beneficial Owner is identified as a foreign PEP:</p>	<p>Where a designated service is being provided to a customer who is, or whose Beneficial Owner is, a foreign politically exposed person, the AML/CTF CO must:</p> <p>(c) obtain any further KYC Information or Beneficial Owner information in accordance with the 'Additional KYC Information' requirements above in this table, including where appropriate, taking reasonable measures to identify:</p> <ul style="list-style-type: none"> (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; and <p>(d) seek Director approval for:</p> <ul style="list-style-type: none"> (iii) continuing a business relationship with a customer; (iv) whether a designated service should continue to be provided to the customer;

	(e) consider whether any of the other measures outlined above are appropriate and should be conducted with respect to the customer who is, or whose Beneficial Owner is, a foreign PEP.
--	---

Issued by the Director of iTeller Pty Ltd

27 June 2023.