ANTI-MONEY LAUNDERING/ COUNTER TERRORISM FINANCING PROGRAM

MoneyPars PTY LTD

297C Prospect Road, Blair Athol SA 5084

Contents

AML/CTF - MoneyPars policy

Introduction and scope

This Program is written to comply with the requirement under the *Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006* ("**the Act**") to have a written AML/CTF Program. It is comprised of Part A: General, and Part B: Customer Identification Procedures.

MoneyPars (the company) is a money transfer service company; this company is a Reporting Entity proving designated services under the Act. The Act imposes certain obligations on Reporting Entities to identify, mitigate, and manage the risk that the provided designated service might involve or facilitate money laundering, terrorist financing or other criminal activity. In addition to various recordkeeping and reporting requirements, The Act requires Reporting Entities to establish and maintain an Anti-Money Laundering/Counter-Terrorism (AML/CTF) Program ("the Program").

As with any Remitter and financial institution, there is a risk of MoneyPars products and services being used to launder money and finance terrorism. Australian law and applicable local laws in the jurisdictions in which we operate, requires us to put training, processes and systems in place to identify, manage and mitigate this risk. We do this to protect the MoneyPars reputation, to comply with relevant laws and to be a good corporate citizen. Failure to do so may result in social harm, significant penalties, including legal and regulatory action.

This Program, and any new versions of this Program, must be retained by the Reporting Entity for 7 years after the relevant version of the Program has been superseded. Appendices 1 and 2 contain additional operational policies, procedures and forms which supplement the Program outlined in this document. Together these document from the compliance manual ("**the Manual**").

MoneyPars requires its directors and employees to comply with Part A and B and the procedures set out in the Appendices.

Our AML/CTF policy

- Sets out how the MoneyPars complies with its legislative obligations
- Applies to all business divisions and employees (permanent, temporary and third party providers) working in Australia and overseas.

Definitions

Money laundering is the process of concealing sources of money. Money evidently gained through crime is "dirty" money, and money that has been "laundered" to appear as if it came from a legitimate source is "clean" money. Money can be laundered by many methods, which vary in complexity and sophistication. Money laundering reduces the risk of detection and confiscation by authorities. It is just as serious as the criminal activity behind it – and preventing it can help reduce crime.

What is Terrorist Financing? United Nations 1999 International Convention for the Suppression of the Financing of Terrorism explains terrorist financing in the following way: ""Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act."

Terrorism financing differs from money laundering in 3 main ways:

- Its primary purpose is to disguise the ultimate use of the funds, as opposed to their origin
- It can involve relatively small sums of money, which can have a huge impact in terms of death, destruction and disruption
- Although terrorists may finance their activities through crime, legitimate funds can also be misappropriated to finance terrorism.

AML/CTF

Means anti-money laundering and counter-terrorism financing

AML/CTF Act / The Act

Means the Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Designated service

Means the services designated in section 6 of the Act

E- currency

Means an Internet-based, electronic means of exchange that is known as any of the following:

- e-currency;
- e-money;
- (eg, electronic transfers but not cheques)

KYC information

Means know your customer information being:

Name, date of birth, residential address

ML/TF

Means Money-Laundering and/or Terrorism Financing

Program

Means the AML/CTF program prepared by MoneyPars Pty Ltd

Reliable and independent KYC documentation/ KYC documentation

Means the documents listed in Part B of this program

Rules

Means the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007(No. 1)

Suspicious matters

Has the meaning set out in Part A of this program

Customer Identification

The AML/CTF Act provides a list of 'designated services', such as opening an account or making a deposit. Before receiving any of these designated services, customers will be required to provide proof of identity or similar documentation.

MoneyPars is required to collect and verify this information, depending on the type of customer:

- **Personal** - an individual person of any nationality
- **A sole trader** - a person who trades in their own legal right without the use of a company structure, incorporation or partners and who, alone, has full liability for the activities of the business
- **Domestic company** - incorporated in Australia, including proprietary, public and listed public companies
- **Foreign company** incorporated outside Australia
- **Partnership** - a relationship between persons (the partners) carrying on business in common, under a partnership agreement, with a view to profit
- **Trust** - a relationship where the trustee holds property or assets for a beneficiary. The trustee can be an individual, a group of individuals or a company.
- **Association** - a group of persons who have agreed to join together in pursuit of one or more common objectives. An association can be incorporated or unincorporated.
- **Registered co-operative** - a legal entity owned and controlled by the people for whom it was established and who benefit from using its services
- **Government body** - can be domestic (e.g. Commonwealth, State, and Territory) or foreign government body.

Suspicion

Money laundering and terrorism financing (ML/TF) are sometimes detected because a customer acts or behaves in a suspicious way.

For a 'suspicion' to be valid, we must have reasonable grounds to believe ML/TF activity may be occurring. To support this, employees receive training in identifying and reporting suspicious matters.

MoneyPars's 5 key AML/CTF principles

1. Comply with AML/CTF legislation in the countries we operate in
2. Fulfil international standards as detailed in the recommendations of the Financial Action Task Force (FATF)
3. Work in conjunction with the Australian Government and the governments of the countries we operate in, and support their objectives in relation to the prevention, detection and control of ML/TF
4. MoneyPars may decide not to provide products or services based upon decisions guided by ML/TF risk appetite and corporate social responsibility
5. Maintain and comply with an AML/CTF program, as required by Australian AML/CTF legislation.

Policy roles and responsibilities

MoneyPars Director and compliance officer have ongoing oversight of AML/CTF policy and procedures. All permanent and temporary employees must comply with these, attend training specific to their role, and report suspicious matters or behaviours.

MoneyPars's AML/CTF program

The design and implementation of the program was tailored to AML/CTF risk profile, applying specific systems and controls, including:

- AML/CTF risk assessment
- Employee training
- Employee due diligence
- customer due diligence
- Transaction monitoring

Monitoring and reporting

We also report the following information to AUSTRAC, Australia’s AML/CTF regulator:

- Transactions with a cash component of AUD10,000 or more
- Electronic transfers of funds into or out of Australia
- Any transactions or other activities regarded as suspicious.

Part A – General

Oversight by boards and senior management

Part A of the Program must be approved and overseen by the governing board (or chief executive officer or owners where there is no board) and senior managers of the company. Approval/adoption is evidenced by signing and dating the first page of the AML/CTF Program.

Oversight is achieved through day to day management of the company and through reports made by AUSTRAC, independent reviewers and/or the Compliance Officer.

Risk assessment

MoneyPars conducts a risk assessment in relation to remittance services provided through its network. This risk assessment, including a description of mitigating systems and controls, is described in Appendix 3.

MoneyPars will review the impact on money laundering and terrorism financing risk before making any changes to MoneyPars designated services offered through the network, or the method of delivering them. Any change in the level of risk, and related changes to systems and procedures, will be communicated to the employees', agents or agent where appropriate and required.

AML/CTF Compliance Officer

MoneyPars designate a person as the AML/CTF Compliance Officer at management level. Particular procedures regarding the appointment of the Compliance Officer are set out in Appendix 1.2.

The Compliance Officer works with management to ensure their ongoing oversight of the Program through implementing policies, procedures and internal controls to correct any compliance deficiencies, enhance compliance performance, and respond to regulatory changes.

The Compliance Officer has the overall responsibility for maintaining compliance with the Agent's AML/CTF Program, including any supporting polices or procedures, and with the Act with the following specific responsibilities:

1. Education of employees on observable customer behaviors that could warrant Suspicious Matter Reports (**SMR**).
2. Ensuring that employees identify and refer/report suspicious activity for both completed and attempted transactions to the Compliance Officer.
3. Review of all SMRs for accuracy and completeness before referring them to MoneyPars (using the SMR referral process set out in Appendix 1.3) for submission by MoneyPars to AUSTRAC.

4. Periodic review of daily reports, forms and/or printed receipts to ensure proper completion and accurate entry of customer information, as well as proper identification acceptance by Agent employees.
5. Monitoring of employee compliance with policies and procedures.
6. Development and implementation of appropriate corrective action for any deficiencies identified during the monitoring process.
7. Ensuring employee due diligence practices is followed and records kept.
8. Ensuring training is completed and records kept.
9. Ensuring independent reviews are completed and that any corrective actions are undertaken and completed.
10. Reporting to management, owners, board (as applies) on compliance generally with this program, including outcomes from reviews to ensure oversight is achieved.
11. Serving as the primary contact between the employee and AUSTRAC, MoneyPars, and Government officials during regulatory audits, registration/enrolment or compliance examinations.
12. Managing any AUSTRAC feedback, taking action upon that feedback and keeping records for 7 years. Sharing information regarding AUSTRAC regulatory comment or action with the MoneyPars compliance team in South Australia.
13. Assisting management in the completion of the annual compliance report.

Ongoing Customer Due Diligence Transaction Monitoring

Under the AML/CTF legislation, MoneyPars has responsibility to conduct ongoing customer due diligence. All monitoring of MoneyPars transactions and consequential suspicious matter reporting is completed by MoneyPars. Further detailed documentation relating to the transaction monitoring program is held by MoneyPars.

Enhanced Customer Due Diligence

Under the Act, MoneyPars is required to apply an enhanced customer due diligence program in relation to an existing customer when it determines that money laundering or terrorism financing risk is high or a suspicious matter report has been made in respect of the customer.

However, because customer identification is performed at every transaction, MoneyPars has determined that collecting further KYC (Know Your Customer) information or verification or updating of KYC generally is not required except where more information is collected at certain thresholds, for example for purpose, occupation and large principle money transfers.

Suspicious Matter Reporting

MoneyPars submits SMRs to AUSTRAC for itself and on behalf of its network. In relation to this, MoneyPars identifies SMRs through its transaction monitoring program (mentioned above), *but the employee or agent remains responsible for identifying its own SMR in relation to any suspicions which arise from face-to-face interactions with the customer.* MoneyPars will, through its Compliance Officer, send an SMR referral whenever it has reasonable grounds to suspect that:

- Customers are not who they say they are, or
- Information about a transaction, attempted transaction or pattern of transactions may be relevant to the investigation of:
    - tax evasion;
    - money laundering; or
    - terrorism financing

Suspicious matters include but are not limited to:

- Possible attempts to launder money, including attempted but not completed transactions;
- Structuring/splitting transactions to avoid reporting and record keeping requirements;
- Observed transactions that are unusual for the customer or serve no business or apparent lawful purpose;
- Altered, questionable or false identification; and
- Inconsistent information with no reasonable explanation

1. All employees are responsible for exercising reasonable diligence in identifying potentially suspicious matters. If an employee becomes aware of activity that he or she believes is suspicious, he or she must notify the Compliance Officer as soon as possible.

2. The Compliance Officer is responsible for determining whether a SMR referral form should be filed with respect to any potentially suspicious activity. The procedure for filing an SMR referral to MoneyPars is set out in Appendix 1.3.

3. Both employees and the Compliance Officer should attempt to obtain as much information as possible about the suspicious transaction(s), including information about the customer or customers involved, and any other identity information that might assist (eg whether to copy a document or not), in order to assist in preparing the SMR. However, they should be careful not to tip off the customer that a referral is being completed. If you think that the customer will be tipped off to your suspicions, do not ask additional questions.

4. The Compliance Officer will retain a copy of the completed SMR referral form along with any supporting documentation for 7 years. Copies of the completed forms must be retained in a way to ensure that they remain confidential (e.g., in a locked drawer).

5. All SMRs are considered strictly confidential and cannot be disclosed to or shared with anyone except the appropriate governmental agencies and law enforcement authorities. Under no circumstances may an employee inform a customer that a Suspicious Matter Report is being submitted.

6. MoneyPars has a separately documented internal process for receiving the SMR referral and any supporting documents and then submitting these to AUSTRAC.

Employee Due Diligence

Any employee must be screened before being able to conduct MoneyPars transactions.

1. Family

Where family and close friends are employed to conduct MoneyPars transactions, their appointment must be personally endorsed by one or more of the signatories to this document based on personal knowledge and satisfaction of the employees background.

2. Other employees

Where an employee is not personally known to the signatories to the Program, the person must produce acceptable and valid photographic identification and must have a minimum of 2 independent background checks completed, and information retained on file while the employee continues to conduct MoneyPars transactions.

Acceptable checks include:

- Previous employment reference checks
- Personal reference checks
- Community type reference checks

The checks will include sufficient research to be satisfied that the person does not pose a money laundering or terrorism financing risk to the business.

Criminal history checks may also be conducted depending on the outcome of the above checks.

3. MoneyPars staff

MoneyPars screens its staff who support the Program (e.g., for reporting on behalf of the Agent, or for approving Large Principal Money Transactions). Details of these screening procedures are held by MoneyPars. These checks include criminal history checks and detailed background checks conducted by MoneyPars human resources personnel.

4. Dealing with non-compliance

When any person is identified as not complying with the requirements of this program or MoneyPars procedures, whether they are employees of the agent or MoneyPars, that person will receive additional training and coaching from the Compliance Officer or manager, or MoneyPars compliance staff. Where non-compliant activities continue the person will be prohibited from conducting MoneyPars transactions, or in the case of MoneyPars staff, be subject to internal MoneyPars disciplinary procedures, which may include termination.

Employee Training

1. Initial Training

AML/CTF Compliance training will be done by all new employees before allowing them to conduct MoneyPars transactions. The Compliance Officer is responsible for ensuring that the training of each employee has been completed and properly documented.

2. Ongoing Training

On an ongoing basis, MoneyPars is required to complete AML/CTF refresher training each year through a variety of formats.

The Compliance Officer is responsible for ensuring all employees and agents receive ongoing training and retain records for 7 years. Likewise, the Compliance Officers provides supplemental training, as needed, to address and to correct any compliance deficiencies noted through monitoring and audit activities.

3. Content of Training

The purpose of the initial and ongoing training is to enable the employees to understand:

- the MoneyPars obligations under the Act and associated rules;
- the consequences of non-compliance with those (both for the Agent and the employee);

- the type of money laundering/terrorism financing risk the Agent/employees might face and the potential consequences of that risk; and
- MoneyPars procedures regarding the provision of MoneyPars services, including procedures under this program

More detailed information about the training programs are set out in Appendix 1.4.

Independent Review

1. Every 2 years, the Compliance Officer will arrange to have the Program independently reviewed to assess:
   - the effectiveness of Part A having regard to the ML/TF risk of MoneyPars;
   - whether Part A complies with the AML/CTF Rules;
   - whether Part A has been effectively implemented; and
   - whether MoneyPars has complied with the program.
2. The Compliance Officer will complete any required corrective actions as soon as possible after the review and will document the corrective actions taken. A report of the review and corrective action will be provided to the board/senior management.
3. Further detail about the Independent Review is set out in Appendix 1.5.

AUSTRAC Feedback

The Compliance Officer is responsible for:

1. coordinating feedback by AUSTRAC and responding to requests for information from AUSTRAC;
2. notifying the board and/or senior management of any AUSTRAC feedback that has been provided;
3. documenting and addressing any audit issues identified in the feedback from AUSTRAC.
4. Documented issues and resolutions will be retained for 7 years;
5. advising MoneyPars compliance staff on any adverse or material matters raised by AUSTRAC; and
6. following up on any corrective action that is required as a result of audit.

Please see the form in Appendix 2.

Reporting Requirements

When must the company make a report to AUSTRAC?

a) Periodically as directed by AUSTRAC
b) Compliance report in March
c) When there is a cash pay-out of ≥$10,000
d) When there is a suspicious matter

Other reporting obligations under the Act SMR 8.9

International Funds Transfer Instructions (IFTI) Reports

MoneyPars's rules-based, automated transaction monitoring system is designed to identify and report, individual money transfer transactions conducted through MoneyPars Pty Ltd originating in Australia and paid outside Australia and vice versa.

The procedures are contained in separate materials developed and maintained by MoneyPars.

Threshold Transaction Reports
Transactions involving amounts of over AUD$10,000 in cash are required to be reported to AUSTRAC. Where cash payments are made over this amount reports will be lodged with AUSTRAC.

Compliance Reports
As a reporting entity MoneyPars is required to complete compliance reports under section 47 of the Act. The specific requirements of these reports are determined by AUSTRAC in relevant Rules.

Part B – Customer Identification

MoneyPars employees and Agents only accept transactions to be sent and received by individuals on their own behalf. For every transaction a customer is required to produce valid identity documents as described below, so that verification of his or her identity can occur.

For every money transfer transaction, employees must:

1. Ensure that at a minimum the following information has been *collected* from the customer:
    - Customer's full name
    - Date of birth
    - Country of birth
    - Physical address (No PO Box address)
    - Purpose of transactions (for transfers of $1,000 or more)
    - Occupation (for transfers of $10,000 or more)
2. *Verify* the full name and either address or date of birth, by reviewing an acceptable form of customer identification and ensure that the identification:
    - Is currently valid (i.e. has not expired)
    - Is government-issued
    - Contains a photograph of the customer who is in front of you
    - Contains the customer's full name
    - Contains the customer's date of birth
3. Accept only the forms of identification acceptable by MoneyPars policy. Examples of acceptable forms of identification include the following:
    - Australian or foreign passport
    - Foreign national identity document/card
    - Australian and foreign driver's license
    - Proof of age card, photo card issued under other state laws

If the identification is not in English, it should be accompanied by an English translation by an accredited translator, unless it is in a language that the Agent/employee is both fluent and literate.

The photograph, name and date of birth must be matched with the ID as above **and where there are discrepancies between the name written on the form and the name on the ID, the name on the form must be corrected to match the name on the ID before entering into the system.**

4. Look at and handle the customer's ID to verify the customer's identify and the ID's authenticity. If an ID is not provided, does not match the customer, or appears to be counterfeit, the employee will refuse the transaction and report the matter to the Compliance Officer for lodging of an SMR referral. **Photocopies of ID documents are not acceptable.**
5. Ensure that the customer has signed the Send or Receive form/Receipt
6. Retain a copy of the Send or Receive form/Receipt. All such copies will be retained for 7 years.

Special identification procedures
Large Principal Money Transfer

Where the amount to be transferred is above a threshold set by MoneyPars (currently $20,000 AUD), additional information is collected from the customer, and must be approved by Department of Foreign Affair and Trade (DFAT) before it can proceed, due to the increased money-laundering and terrorism financing risk associated with the transaction.

A detailed procedure regarding Large Principal Money Transfers is set out in Appendix 1.6.

Other important information:

- Transactions must always be conducted in person by an **individual** who is identified and verified as above. Where the individual is also a **sole trader** then you must also collect the following information and enter it into the system:

Collect	Record
Australian Business Number (ABN); and	ABN field in Customer Info of Translink/ID Details of WU POS
Trading name of the Sole Trader's business; (e.g. John Smith Plumbing)	Comments field

- Third party transactions are not permitted. The person sending the transaction must be the person on the form with the right identification.
- Under no circumstances should employees allow amounts to be split to avoid reporting thresholds ($10,000).

Privacy

All entities are now subject to the Privacy Act in relation to the handling of information under the Act (except for suspicious matters).

In summary the Privacy Act requirements are:

- Only collect the information the company needs in order to comply with the program
- Advise the person of the use to which the information will be put. eg when the company collects KYC information in accordance with Part B, the company should tell the customer that the information will be kept for the purposes of the AML/CTF Act (but NOT suspicious matters)
- Do not disclose the KYC information to any unauthorised persons, eg marketing companies, without obtaining specific consent from the customer first
- Take reasonable steps to ensure that the KYC information is correct and up to date
- Store the register and any copies of KYC documentation in a manner which protects it from misuse, loss or unauthorised access
- Destroy the KYC entries and documentation after 7 years
- Provide the customer with access to the information that relates to the customer (but NOT suspicious matters)
- Correct any false information relating to the customer

Suspicious matters are not subject to the Privacy Act. Any information collected and recorded in response to a suspicious matter cannot be disclosed to anyone other than to AUSTRAC. If the information is disclosed, in particular to the person/s noted in the suspicious matter report, the company and the person who does the tipping off will be breaching the tipping off laws and liable for penalties.

APPENDIX 1 - Procedures

1. Oversight by boards and senior management

a) The owners of the MoneyPars should provide copies of this Program document to all members of the board and/or to senior management overseeing the business.

b) Members of the board and/or senior management should review and understand the policies outlined in Parts A & B of this document.

c) Additional clarification should be provided as needed by the MoneyPars Compliance staff.

d) After final approval of the policies outlined in Parts A & B, members of the board and/or senior management should sign and date the title page of this document.

e) A copy of this approved document should be retained at each location of the MoneyPars for 7 years.

f) Board and/or senior management should continue to oversee the compliance with the program by requiring updates and information from the Compliance Officer on any material matters such as results of audits, contact by independent person, or contact by regulators or law enforcement.

g) The procedure outlined above should be applied in relation to any variation to or new version of this Program that is adopted by MoneyPars.

2. AML/CTF Compliance Officer

a) MoneyPars management should determine a suitable employee at management level to be designated as Compliance Officer. That person can have other duties as well as his or her duties as Compliance Officer.

b) The designated Compliance Officer should review and thoroughly understand the content of Parts A & B of this Program document, including especially Section III of Part A.

c) Additional training, as determined management, should be provided to the designated Compliance Officer.

d) The designated Compliance Officer should sign and date the designated compliance officer form in Appendix 2 upon acceptance of and understanding the role.

3. Suspicious Matter Report Referral Procedure

a) A Suspicious Matter Report Referral form must be submitted to compliance officer for any completed or attempted transaction for which there is a reasonable basis to suspect that the transaction or attempted transaction is related to tax evasion, illegal activity, money laundering or a terrorist financing offence, or where the customer is not who they say they are. A copy of the Suspicious Matter Report form is located in Appendix 2. THIS INFORMATION MUST COME TO COMPLIANCE OFFICER FOR REVIEW AND SUBMISSION TO AUSTRAC.

b) Suspicious Matter Reports are to be reviewed for completeness and accuracy by the Compliance Officer prior to submission to AUSTRAC. The referral form may be amended

from time to time by MoneyPars for administrative purposes only as it deems necessary to meet its regulatory and legal obligations. MoneyPars will not form any view on, approve or otherwise, the suspicion you raise.

c) The Compliance Officer will submit the report within the applicable statutory timeframes to AUSTRAC.

d) The Compliance Officer will serve as the contact person should AUSTRAC have any questions about Suspicious Matter Report.

e) Copies of Suspicious Matter Reports and evidence of submission to AUSTRAC, along with all supporting information, must be retained for a period of 7 years.

4. Employee Training

a) Initial Training

i) To satisfy initial training requirements, each employee will complete face to face or online training offered through MoneyPars. The Compliance Officer may receive additional training.

ii) Online training offered through MoneyPars also allows for record keeping.

iii) The Compliance Officer will confirm that training of each employee has been completed in a timely fashion and properly documented, and retain training records for 7 years.

b) Ongoing Training

i) Every year MoneyPars agents and employees are required to receive AML/CTF refresher training by one or more of the following ·

(1) Completing online training modules again;

(2) Completing AUSTRAC training;

(3) Attending regional conferences;

(4) Viewing webcast presentations;

(5) Reading MoneyPars or other AML publications;

(6) Participating in agent outreach programs when they are conducted;

(7) Participating in training calls;

(8) Participating in offsite and onsite program reviews.

ii) In addition, the Compliance Officers provides supplemental training, as needed, to address and to correct any compliance deficiencies noted through monitoring and audit activities.

iii) The Compliance Officer will document completed ongoing training, and retain records for 7 years.

iv) See Appendix 2 for a sample training log form that may choose to use for ongoing training records.

5. Independent Review

a) Once every two years the AML/CTF Compliance Officer will arrange to have the AML/CTF Program independently reviewed. The independent review must address the issues set out in Part 8.6 of the AML/CTF Rules (set out in Part VIII of Part A AML/CTF Program).

b) The review will be carried out by a suitably qualified person who has AML/CTF training and is either an internal party or an external party independent;

c) The Compliance Officer may not serve as the reviewer, nor may the reviewer be a subordinate of the Compliance Officer.

d) The MoneyPars independent review template (see Appendix 2) will be used to conduct the review

e) The Compliance Officer will ensure the completion of any required corrective actions as soon as possible after the review, and will document the corrective actions taken by management and Agent.

f) Copies of all Independent Reviews and any documented corrective actions will be provided to the governing board and/or senior management and will be retained for 7 years.

6. Large Principal Money Transfers (LPMT)

To ensure a prompt response to any LPMT request, it is important to get all the facts about the transaction, obtain supporting documentation and accurately complete the LPMT form before contacting OSAS online. The LPMT form is located in Appendix 2 of this document.

Employees must take reasonable measures to obtain as much information as possible for completion of the LPMT form. The procedure is as follows:

a) Determine the purpose of the transaction. If there is uncertainty about the purpose of the transaction, ask the customer open-ended questions. Examples of questions that may need to be asked are: “what is the purpose of the transaction, source and origin of the funds”. “can you tell me the senders relationship to the receiver,” “ what previous dealings with the receiver have you had?” .

b) Check whether the paying agent can offer the requested payout amount. This can be done by checking Country Information of the destination country. For example: the payout restriction in India is USD 2,500 per transaction.

c) Obtain supporting documentation to justify the purpose of the transaction and the origin of the funds.

d) Ensure the customer completes the LPMT form or email the information.

e) Review the LPMT forms for completeness and accuracy prior to submission to MoneyPars. The MoneyPars Operator Complete OSAS on line form, and all supporting documentation directly to the OSAS on Line. For email/fax contact details, please refer to the LPMT form located in Appendix 2.

f) The MoneyPars Agent Support Line will then process the request and obtain all necessary approvals for the transaction to proceed.

g) Copies of the LPMT forms and all supporting documents must be retained as per normal record keeping procedures, for a period of 7 years.

Examples of when a LPMT would be accepted or refused:

a) Accepted:

   i) Payment for urgent surgery.

   ii) Payment for funeral expenses.

   iii) Family Support.

   iv) Legal Fees.

   v) Tuition Fees.

   vi) The customer must provide supportive documentation in order for a transaction to be accepted.

b) Refused:

   i) Payment for personal business, where sender unable to provide supportive documents.

   ii) Gambling.

   iii) Investment Purposes.

   iv) To purchase stocks, bonds, gold, silver, minerals.

APPENDIX 2 - Forms

Designation of Compliance Officer

Name: _____

Role accepted (signature) _____

Date Assigned: _____

Date Removed: _____

Name: _____

Role accepted (signature) _____

Date Assigned: _____

Date Removed: _____

Name: _____

Role accepted (signature) _____

Date Assigned: _____

Date Removed: _____

LARGE PRINCIPAL MONEY TRANSFER FORM

For use with transfers exceeding AUD 20,000	Please send the completed LPMT form and supporting documents to MoneyPars on (08) 8269 1745 or email to info@MoneyPars.com with email subject: **LPMT**

Transaction Information:

Send Amount:	Local Currency:
Destination City/Country:	Expected Payout Date:
Purpose of Transfer:	
Source of Funds:	
Has the Sender ever sent a MoneyPars Money Transfer before?	
Is the Sender aware of the fee and F/X rate and agrees to them?	
Have you checked for any restrictions in the Send/Pay country that would NOT allow for this amount to be sent?	

Sender Information:

Sender Name:	First:	Last:
Sender's Address:	Street address:	City:
Indicate type and number of ID presented (**mandatory**)	ID type	ID Number:
Bank account details:		

Payee Information:

Payee Name:	First	Last:
Payee's Address:	Street address:	City
Bank Account Details:		

FOR MONEYPARS USE ONLY

Paying Agent Information:

Has Paying Agent been contacted and agrees to payout the Money Transfer?	
Payout location (if known):	
Authorization for payout given by:	
Network Agent:	Operator (name & ID)
Approved by:	Date:
Declined by: Reason of declension:	Date:
Account No:	
Comments	

Independent Program review

To ensure our Compliance Program is adequate and maintained, we are required to periodically conduct an Independent Review. MoneyPars suggests that the Independent Reviewer be an accountant or attorney, or suitable 'independent' person who has received training in AML Compliance. The reviewer may NOT be a subordinate of the Compliance Officer. The Review should be completed at least every two years and this form (or an equally suitable form) may be used. To use this form in completing the Independent Review of our AML Compliance Program**:**

Independent Review Checklist

Please ensure the Independent Review Checklist is completed once every 2 years and kept on file for at least 7 years.

Date of last review: _____

Review Period:

	Review Procedure	Yes	No	Comments
COMPLIANCE OFFICER POSITION				
1	Has a Compliance Officer been designated for the location?	○	○	
2	Name of Compliance Officer:	**Answer:**		
3	Does the Compliance Officer have written duties and responsibilities in addition to those in the AML/CTF Agent Compliance Program?	○	○	
4	Is the Compliance Officer aware of the procedures and equipped to handle AUSTRAC feedback? Review and comment on any AUSTRAC feedback, actions, activities and records.	○	○	
5	Does the Compliance Officer carry out the duties and responsibilities as outlined in the AML/CTF Compliance Program Manual? Briefly describe routine tasks carried about as described by the Compliance Officer.	○	○	
PART A PROGRAM REVIEW				
6	Is the Business' AML/CTF Compliance Program in a written form and kept at the business location? Provide comments if you sighted it.	○	○	
7	Has the AML/CTF Compliance Program (and any changes) been approved and signed off by the Board/Senior Management?	○	○	
8	Have the AML/CTF Compliance Program's policies and procedures been communicated to all authorised employees conducting MoneyPars transactions? Please comment on When was it/is this done and/or how often it is updated.	○	○	
9	Has any previous AML Program been archived for 7 Years? If Yes, please comment on where.	○	○	
MONITORING				
10	Is monitoring of observable transactions for suspicious behavior being conducted on a regular basis?	○	○	
11	How often is monitoring of forms, records, ID collection, and SMR referrals being conducted?	Daily ○	Weekly ○	Monthly

		○ Other_____		
12	Are identified compliance deficiencies addressed in a timely and effective manner?	○	○	
13	Is monitoring being documented (i.e. Monitoring Checklist)?	○	○	
14	How is monitoring documented?			
15	Is monitoring documented for at least 7 years?	○	○	
16	Is monitoring etc. fed back to Management or the Board to ensure oversight?	○	○	

TRAINING

17	During the review period, have new hired employees received initial AML/CTF Compliance training? If yes, indicate how in the Comments section.	○	○	
18	Have all existing employees (including the Compliance Officer), received initial AML/CTF Compliance training?	○	○	
19	Is initial AML/CTF Compliance training being documented? If yes, indicate how in the Comments section.	○	○	
20	Have all employees, including the Compliance Officer, received AML/CTF Compliance ongoing training?	○	○	
21	Is AML/CTF Compliance ongoing training being documented? If yes, indicate how in the Comments section.	○	○	
22	Interview at least one employee who conducts MoneyPars transactions. Based on interviews with employees who conduct MoneyPars transactions; do employees understand the compliance policies and procedures relating to AML/CTF laws and the Anti-Money Laundering and Counter-Terrorism Financing Act?	○	○	
23	Name of employee interviewed:	**Answer:**		
24	How is the Business' AML/CTF Compliance training program kept current? Explain.	**Answer:**		
25	Is AML/CTF Compliance training documentation being retained for at least 7 years?	○	○	
SUSPICIOUS MATTER REPORTS **Review SMR referral forms completed and submitted during review period.**				
26	Have there been any unusual or suspicious transactions identified during this review period? **If yes, continue with steps 27-28. If not, go to step 29.**	○	○	

27	Are SMR forms properly completed and submitted to MoneyPars immediately after the detection of the suspicious activity?	○	○	
28	Are all SMR forms and their back up documentation being retained for at least 7 years?	○	○	
CUSTOMER IDENTIFICATION & RECORDS				
29	Are ID identification policies (including LPMT reports) being appropriately followed?	○	○	
30	Do you allow third party transactions at your location?	○	○	
MONEY TRANSFER SEND AND RECEIVE FORMS/RECEIPTS **Review a sample of Money Transfer Send and receive receipts for transactions conducted during the review period.**				
31	Are the Money Transfer records properly completed?	○	○	
32	Are Money Transfer records signed by the customers?	○	○	
33	Are the Money Transfer records maintained for 7 years?	○	○	
EMPLOYEE DUE DILIGENCE & USER CODES				
34	Has the employee due diligence program been sufficient to identify employees who may increase the ML/TF risk? e.g. Have there been any incidents where an employee was involved in ML/TF or other criminal activity, despite having been screened?	○	○	
35	Has employee due diligence been performed in accordance with Part A of the program?	○	○	
36	Does each employee use a unique user code and password when conducting Money Transfer transactions?	○	○	
AUSTRAC FEEDBACK				
37	Has there been any feedback received from AUSTRAC?	○	○	
38	Has proper response been provided to AUSTRAC?	○	○	
39	Are all records related to AUSTRAC feedback and resolutions being kept for 7 years?	○	○	
CORRECTIVE ACTIONS				
40	Have there been any corrective actions during past Independent Reviews?	○	○	
41	Have past corrective actions been implemented?	○	○	
42	Please comment on how is the Management & Board oversight evidenced. Comment on what actions has been taken and when			

	was this last done.	

Please summarise and describe any corrective actions which should be taken by the Business based on this review. If necessary, continue the summary of this page on a blank page.

Independent Reviewer:

First and Last Name Signature

Compliance Officer:

First and Last Name Signature

This review should be provided to Management/Board for oversight purposes.

This review may be sighted by MoneyPars or regulator as required.

Suspicious Matter Report

Money Transfer

Instructions: Please complete this form and email to info@MoneyPars.com within on the same day as the reportable activity took place. Keep this form, the transaction forms (if applicable) and the fax confirmation for 7 years. Please fill in as much information as possible. . **NOTE:** This form is to be used by employees and Agent/Agent who are using the MoneyPars process.

Please choose: (☐Completed ☐Attempted)

A. employee Information

Name _____ **Contact Name** _____

Agent Name _____ **Contact Phone** _____

Address _____ **Referral Date** _____

B. Customer Information (One customer per form)

Last Name			First Name										
Middle Name(s) if any			Date of Birth										
			YEAR							MONTH		DAY	
Address (not a PO Box)					City								
State		Postal Code			Country								
Country of Birth						Phone #							
ID	☐Driver's License ☐Passport ☐Other												
ID		Issuing Prov/Country											
Issue date and/or expiry date Occupation													

D. Information about Transaction(s)

☐Send ☐Receive MTCN: _____ Date _____ Time _____
HH-MM-SS

Originating Country _____ Amount $ _____

Destination Country _____ ☐Cash ☐Debit ☐Other _____

If the transaction was not completed, enter the reason here: _____

_____

Purpose of Transaction:

E. Identification of Suspicious Indicator(s)

Choose the indicator(s) that best describes the situation; complete the notes section with as much detail as possible.

01☐ Customer admits or makes statements about involvement in criminal activities.

02☐ Customer offers you money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.

03☐ Customer presents funds for a transaction. Upon request for additional information, he/she decides not to send funds.

04☐ Customer attempts to convince employee not to complete any documentation required for the transaction.

05☐ Customer makes inquiries that would indicate a desire to avoid reporting.

06☐ Customer is quick to volunteer that funds are clean or not being laundered.

07☐ Multiple attempts occur on the same day at the same location but with an apparent attempt to use different employees.

08☐ Customer attempts transactions that are suspicious but seems blind to being involved in money laundering activities.

09☐ Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.

10☐ Customer repeatedly uses an address but frequently changes the names involved.

11☐ Customer uses aliases and a variety of similar but different addresses.

12☐ Customer has unusual knowledge of the law in relation to suspicious transaction reporting.

13☐ Customer seems very conversant with money laundering or terrorist activity financing issues.

14☐ Customer shows uncommon curiosity about internal systems, controls and policies.

15☐ Transaction is unnecessarily complex for its stated purpose.

16☐ Customer attempts to conduct a transaction for an amount that is unusual compared to amounts of past transactions.

17☐ Customer attempts to conduct frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.

18☐ Inconsistencies appear in the customer's presentation of the transaction.

19☐ Customer is involved in activity out-of-keeping for that individual or business.

20☐ Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities.

21☐ Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the customer.

22☐ Activity is inconsistent with what would be expected from declared business.

23☐ Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

24☐ Customer provides doubtful or vague information.

25☐ Customer is accompanied and watched.

26☐ Customer presents confusing details about the transaction.

27☐ Customer over justifies or explains the transaction.

28☐ Customer insists that a transaction be done quickly.

29☐ Customer is nervous, not in keeping with the transaction.

30☐ Customer attempts to develop close rapport with staff.

31☐ Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.

32☐ Customer deposits musty or extremely dirty bills

33☐ Other (please describe):

Notes - provide as much detail and explanation of the situation as possible.

If you were not able to identify the customer by name, please include:

- A description of the person
- Whether you have any photo or video of the person

If the person said that they were acting for someone else, please include:

- Any description of an authorization by the other person for the person to act as agent

Please include any additional information you have which may identify the other end of the transaction (the sender or the recipient, as the case may be), including:

- Name, address (not PO box), telephone number, email

Anti-Money Laundering Compliance Training Log

This AML/CTF Compliance Training log should be kept up to date and on file at the company location for 7 years.

Be sure to fill in all the fields of the log when training is completed.

Next to the "Employee Name", each employee is required to write his or her initials to signify that the indicated compliance training has been received.

Business Name and Address: _____

Training Date	Employee Name	Employee Initials	Check off type of training		Type of Training Provided and the Person Providing the Training
			Initial	On-going	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	
			○	○	

FEEDBACK FROM AUSTRAC

The company may receive feedback from AUSTRAC in response to a report about a suspicious matter or a payment or on the appropriateness of the company's program. The company must respond to any feedback from AUSTRAC in the manner specified by AUSTRAC.

Date feedback received from AUSTRAC: _____

Action required: _____
_____
_____
_____
_____
_____
_____

Date action undertaken: _____

APPENDIX 3 - Risk Assessment

MONEYPARS ANTI-MONEY LAUNDERING and COUNTER-TERRORISM RISK ASSESSMENT ("Risk Assessment")

Overview and Objectives

MoneyPars Pty Ltd ("MoneyPars" or "Company") has prepared this Anti-Money Laundering and Counter-Terrorism ("AML/CTF") Risk Assessment to identify the major AML/CTF risks, mitigation strategies and residual risks in Australia for itself.This document will serve to direct and focus the efforts of MoneyPars larger AML/CTF program headed by the Company's Customer Protection, Compliance and Ethics Office ("AML Compliance").

Scope: This Risk Assessment will focus on the company AML/CTF risks and efforts in Australia for use in MoneyPars AML/CTF Program.

Methodology Overview: MoneyPars takes a risk-based approach in mitigating AML/CTF risk following AUSTRAC guidelines which emphasise the need for money services businesses ("MSBs") to take this type of approach. As stated in the AUSTRAC guidelines:

Adopting a risk-based approach implies the adoption of a risk management process for dealing with money laundering and terrorist financing. This process encompasses recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks.

This Risk Assessment analyses risk across three broadly defined categories using a mix of qualitative and quantitative factors where relevant:

- Customers
- Geography
- Services

MoneyPars considers the assessment and mitigation of risk to be an ongoing and dynamic process. As such, this Risk Assessment represents a snapshot of the Company's efforts as of the date of this document. Where relevant, future plans, challenges and areas of improvement will be noted and discussed.

For ease of understanding, MoneyPars's efforts, policies, procedures, programs, controls and systems will be discussed at a high-level. Additional information is available upon request.

Overview and Objectives

Several regulatory guidelines, as well as the guidelines issued by AUSTRAC emphasise the need for a risk-based approach to controlling AML/CTF risk.

One risk category of a comprehensive risk assessment is the assessment of a money service business' customers.

- MoneyPars provides Services to customers throughout the world,
- MoneyPars provides customers with choices, convenience and control through its Services available via walk-in to company and Agent locations

The steps to assess Customer risk are the evaluation of:

- **Inherent Risk:** The general risk exposure that would exist or arise in the absence of controls designed to mitigate the risk;
- **Mitigation Strategies:** The controls, limitations or processes that should reduce the likelihood of occurrence of a potential event, the impact of an event, or both; and
- **Residual Risk:** The risk remaining after implementation of the controls.

Inherent Risk

Money Transfer Services:MoneyPars's inherent customer risk is the risk that criminal actors will use MoneyPars services to further their illegal activities. MoneyPars identifies customer risk based on why and how illegal customers may misuse Services and the inherent challenges in identifying and stopping this behavior.

Risk arising from Transaction-Based Interaction: MoneyPars provides Services to customers on a per-transaction basis. Consequently, customers who wish to misuse Services can attempt to mask their behavior through use of inconsistent or fraudulent biographical data or transactional patterns. Transactions conducted by the same or related people are not obvious without additional work and data aggregation. Further, legitimate customers can use different biographical data by mistake or due to personal preference (e.g. the use of a middle name) and may have data similar to other customers. Finally, MoneyPars has no ability to verify the biographical information of a customer beyond sighting photographic identification.

Mitigation Strategies:

The Program employs multiple systems and controls to mitigate risk from a customer perspective.

Point-of-Sale Controls: The below controls are effective when a customer first comes into company location or uses the Company's Internet site. At this point of a transaction no money has changed hands and the transaction is not considered to have taken place.

Due Diligence - employee must obtain, verify and record certain customer information as required by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and MoneyPars's own internal policies. Data collection requirements increase as the amount of the transaction increases.

Large Principal Money Transfers - At certain higher dollar thresholds a sending customer will be subjected to the collection of further specific information and documentation by the employee. Before a LPMT transaction is sent, a MoneyPars Customer Representative will check to see if the sender is a politically Exposed Person (PEP) and conduct a review. The Customer Service Representative will work to ascertain the nature of the transaction, the source of the funds, and the sender's relationship to the receiver.

Agent and Employees Training – MoneyPars provides its agents and employees with training (unless they use their own training) and resources to identify customers of higher risk and to take appropriate action

Post-Initiation Controls**:** Post-Initiation controls act after a transaction is finalised at the point-of-sale but before the transaction is completed by payment to a recipient.

Government Sanctions: **MoneyPars's Government Sanctions Program systematically screens and compares names and biographical information provided for a transaction against various lists provided by Australian government. If there is a match against one of these lists, the transaction is not allowed to be completed and appropriate action is taken as required by law.**

Interdiction Screening*:* This program stops transactions from being paid when the sender or receiver of the transaction is identified as a customer who has been placed on a list of interdicted customers.

Ongoing Analysis**:** The following controls are "back-office" controls in that they do not act in real-time and only review transactions that have already been completed.

Transaction Analysis: MoneyPars uses multiple systems to review transactions after they are completed and submits a suspicious matter report those transactions where required. Company also monitor face to face transactions and report suspicions either directly or through the MoneyPars SMR referral process.

Residual Risk

MoneyPars's residual customer risk is ranked as MODERATE due to ever-changing risk of persons wishing to misuse Services and the challenge MoneyPars faces in identifying customers and aggregating their behavior. MoneyPars has a mature, well-developed and agile AML Compliance program but must remain vigilant to adapt to ever-changing customer risk.

GEOGRAPHIC & SERVICES RISK

Overview and Objectives

Several regulatory guidelines, as well as the guidelines issued by AUSTRAC emphasise the need for a money service business to take a risk-based approach to controlling AML/CTF risk.

As part of these efforts, MoneyPars has undertaken a Geographic and Services Risk Assessment

Geographic Risk

Agents can send to wherever the MoneyPars network extends, and therefore all geographic controls are managed by MoneyPars and documented separately. MoneyPars risk ranks countries and territories throughout the world to priorities and direct risk mitigation efforts, Country risk is determined through the combination of externally available data from reputable 3rd parties (e.g. DFAT and AUSTRAC), Internal data (e.g. transactional data, Agent population and mitigation efforts) and measures of transactional risk factors at a country level. These items are combined to generate a comprehensive risk ranking for each country and territory where the Company does business.

Services Risk Agents and employees can only provide services provided by MoneyPars and therefore all product and services controls are managed by MoneyPars and documented separately. In Australia, Agents and employees are only able to offer the Company's money transfer. Beyond those mitigation measures discussed above the Company takes numerous real-time and back-office steps to mitigate risk in its money transfer service. Additionally, Agents and employees are limited as to the volume of transactions they can process (e.g. per day). Overall, MoneyPars ranks this service as a moderate risk due to the availability of Agent locations and the challenge of aggregating customer behavior across multiple days, transactions and agents.

MONITORING AND REVIEW RISK

MoneyPars reviews its risk assessment and mitigation regularly taking into account any changes in the service provided, the customer base, any system changes, and any new tools available to mitigate risk. Any change to the level of assessed risk, as well as any changes to network systems and procedures, is communicated to an employee and Agent as appropriate and required.