



ANTI MONEY LAUNDERING & COUNTER TERRORISM FINANCING POLICY

<i>When updated</i>	<i>Who updated</i>	<i>Details</i>
1 Aug 2014	NS	Revised and improved layout
15 Feb 2017	IJ and NS	Reviewed and reformatted
3 Oct 2019	IJ	ACFID request to reference List of Terrorist Organisations
8 March 2021	NS	Updated to incorporate separate AML & CTF rules
Oct 2021	EH	Reviewed; minor clarifications

Policy/ Manual Name	<i>AML & CTF Policy</i>
Signoff Authority	<i>Board</i>
Owner signoff & date	<i>Financial Controller, Nov 2021</i>
Compliance signoff (if required) & date	<i>n/a</i>
Final signoff & date	<i>Board, Nov 2021</i>
Next review date	<i>2024</i>
Website update required?	<i>n</i>
Training update required?	<i>n</i>

Contents

1 Purpose	2
Part A	3
1.1 Roles and Responsibilities	3
1.2 Glossary	3
1.3 Key Principles	3
1.3.1 Definition of money laundering and terrorism financing	3
1.3.2 Know your Customer (KYC)	3
1.3.3 Know your Employee (KYE)	4
1.3.4 Suspicious activity	4
1.3.5 AML&CTF Training program	4
1.3.6 Record retention	4
1.3.7 Independent review of the AML&CTF Program	4
2 Customer Identification Procedures (CIP)	5
2.1 Customer Risk	5
2.2 Politically Exposed Persons (PEPs)	5
2.3 Jurisdictional Risk	6
2.4 Enhanced Customer Due Diligence (ECDD)	6
2.5 Verification of KYC information	6
2.6 ONGOING CUSTOMER DUE DILIGENCE (OCDD)	6
2.7 Ongoing KYC reviews	7
2.8 Transaction Monitoring Program	7
3 Reporting Obligations	7
3.1 Suspicious Matter Reports (SMRs)	7
3.2 Knowledge and Suspicion	7
3.3 Unusual Activity	8
3.4 Threshold Transactions	8
3.5 Responding to AUSTRAC feedback	8
Appendix A Identification and Verification	9

1 Purpose

This Anti Money Laundering and Counter Terrorism Financing policy summarises the consolidated policies and procedures Good Return has adopted in order to meet its obligations under the Australian Anti Money Laundering and Counter Terrorism Financing Act (2006) (“the Act¹”). The Act requires Good Return to adopt and maintain a risk based AML&CTF Program composed of a Part A and a Part B.

Good Return has received legal advice that it provides two “designated service”, as defined by the Act, as follows:

Item	Provision of a Designated Service	Customer
6	making a loan, where the loan is made in the course of carrying on a loans business	the borrower
7	in the capacity of: (a) lender for a loan; or (b) assignee (whether immediate or otherwise) of the lender for a loan; allowing the borrower to conduct a transaction in relation to the loan, where the loan was made in the course of carrying on a loans business	the borrower

Good Return does not lend directly to individual borrowers. Instead, it makes an interest-free loan to a local partner microfinance institution (MFI) who then lend small amounts to the individual borrower. Good Return’s AML&CTF program is tailored to its situation and money laundering and terrorism financing risks. It assesses the AML&CTF risks posed by its customers and services and allocates appropriate resources to counter those risks. Therefore, Good Return’s focuses on two key risks:

- Customer risk:** the types and the jurisdictions in which they operate (Section 2 below); and
- Delivery risk:** the method by which we deliver the loans to MFI partners (Section 3 below).

Part A of Good Return’s AML&CTF policy is designed to identify, mitigate and manage the risk of money laundering and terrorism financing. Part B sets out the applicable customer identification procedures for the purposes of the application of the Act to our MFI partners.

This policy is designed to provide Good Return’s staff with an understanding of:

- The obligations that it has under the Act and Rules (collectively ‘the rules’)
- The consequences of non-compliance with the Act and Rules
- Types of AML&CTF risks that Good Return faces and potential consequences of such risks
- Good Return’s risk based approach to money laundering and terrorist financing risks
- Good Return’s policies and procedures that are in place to meet AML&CTF obligations
- How to recognise ML/TF and the actions that must be taken if a suspicion is formed.

Policy: Anti Money Laundering and Counter Terrorism Financing (AML& CTF) laws impose obligations on Good Return as a reporting entity, to include:

- **customer identification and verification of identity, and record-keeping.**
- **establishing and maintaining an AML & CTF program.**
- **ongoing customer due diligence and reporting (suspicious matters, threshold transactions and international funds transfers).**

Procedure: With regard to potential partners, Good Return will undertake activities:

- to know which organisations and people that are being assisted, including any searches or checks considered necessary;
- to ensure that directly funded organisations are aware of and obliged to comply with these laws, and in turn are obliged to make sure their distribution of funds is on the same basis.

¹ Section 80, AML/ CTF Act (2006).

Part A

1.1 Roles and Responsibilities

It is the responsibility of all staff to comply with this policy. Failure to do so may result in disciplinary action, including possible dismissal or other sanction.

The CEO is AML&CTF Compliance Officer. This role includes:

- Oversee the design, maintain and review the effectiveness of the AML&CTF program
- Oversee the implementation and operation of AML&CTF systems and controls
- Monitor compliance with the Act and Rules and any changes to these
- Point of escalation for any customers determined to be high risk
- Investigate unusual or suspicious activities
- Coordinate communications with AUSTRAC including reporting
- Provide updates to senior management and the Good Return board.

Under the overview of internal Risk and Compliance advisors, the Financial Controller is the designated AML&CTF Reporting Officer, and is responsible for threshold transaction reporting to AUSTRAC. The Compliance Adviser is responsible for the annual AML Review checklist completion and employee training updates as needed. Management and Board maintain oversight of the program. The Compliance and/or Risk Advisor will review the program at regular intervals.

1.2 Glossary

In this policy the following defined terms are used

AUSTRAC	Australian Transactions Reports and Analysis Centre
AML&CTF	Anti Money Laundering & Counter Terrorism Financing
the Act	Australian Anti Money Laundering & Counter Terrorism Financing Act 2006
CDD	Customer Due Diligence
CIP	Customer Identification Procedure
Designated Service	making a loan, where the loan is made in the course of carrying on a loans business; in the capacity of: lender of a loan; or assignee (immediate or otherwise) of the lender of a loan;
DFAT	Department of Foreign Affairs & Trade
ECDD	Enhanced Customer Due Diligence
Identify	collecting customer information
KYC	Know Your Customer
KYE	Know Your Employee/staff
Terrorist Organisations	the list of terrorist organisations designated as such by Australia and maintained and published by Australian National Security at: https://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/default.aspx
ML/TF	money laundering and terrorism financing
OCDD	Ongoing Customer Due Diligence
PEP	Politically Exposed Person
RE	Reporting Entity
Staff	all persons in Good Return including directors, paid staff and volunteers
Verify	to confirm or prove a fact from reliable and independent source documents.

1.3 Key Principles

1.3.1 Definition of money laundering and terrorism financing

Money Laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Terrorist Financing (TF) is generally the act of providing financial support to terrorism or terrorist organisations to enable them to carry out acts of terrorism. Terrorist financing does not necessarily involve illegitimate funds; in fact it often uses legitimately obtained income and may involve relatively small amounts of money.

1.3.2 Know your Customer (KYC)

Staff must understand and follow all Know Your Customer (“KYC”) policies and procedures relevant to their responsibilities, business and jurisdiction. Applicable KYC policies and procedures to establish and verify identity and bona fides of customers should be understood and complied with.

1.3.3 Know your Employee (KYE)

As staff may be at risk of knowingly or unknowingly facilitating a ML/TF incident, the Act and Rules imposes a number of obligations on Good Return to maintain controls to minimise that risk. The key requirements for KYE are found within Chapter 9 of the AML&CTF Rules Instrument 2007 (No.1). Good Return will undertake the following activities:

- Screening of staff on appointment, transfer or promotion
- Additional screening of directors, officers and key personnel
- The reporting of AML&CTF program breaches by staff.

1.3.4 Suspicious activity

Good Return staff must be aware of red flags, or anything that is unusual or out of the ordinary when dealing with customers and customer related information.

Evidence of potential money laundering or terrorism financing may be obvious. However, in some cases, the suspicious nature of an activity or transaction may be cumulative. Suspicious elements are sometimes referred to as “red flags” and include:

- Reluctance or refusal by a prospective partner to provide reasonable information as requested
- Inadequate information on a MFI partner
- A prospective MFI partner who lacks a banking, business or credit history
- One or more transactions that appear unusual or uncharacteristic considering the MFI's financial profile or history
- Transaction that appears to lack reasonable economic substance or intent
- Transaction that appears to be structured intentionally to evade applicable government reporting or record keeping requirements
- Transaction that seems unnecessarily complex or exceeds the MFI's capacity

These are all general warning signs, and are only intended to provide a broad characterisation of some types of suspicious activity.

In the event staff becomes suspicious in relation to customer activity, they should advise the designated AML&CTF Compliance Officer or in their absence, the CEO. Revealing to anyone outside Good Return including the client, that a suspicion has been formed may breach the law.

1.3.5 AML&CTF Training program

The purpose of our AML&CTF Training Program is to educate staff in implementing and maintaining its AML&CTF Program. It will be provided at regular intervals. Good Return will retain copies of the training provided and of who has been trained.

1.3.6 Record retention

Good Return will retain relevant records for as long as needed by applicable rules and regulations.

1.3.7 Independent review of the AML&CTF Program

Our AML&CTF Program is subject to independent review by the compliance advisor, internal risk manager or other independent party (eg auditor) for effectiveness. The results of the review, including any report prepared, will be presented to management for appropriate action.

Part B

This part relates to its customer identification procedures (CIP) and includes:

- Establishing methods for identifying customers (and their agents), to enable Good Return to be reasonably satisfied that a customer is who they claim to be
- Collecting and verifying KYC information
- Conducting regular cross checks of individuals and entities against the DFAT Consolidated List, World Bank Listing of Ineligible Firms & Individuals and the List of Terrorist Organisations (as updated)

A MFI partner's identity must be verified prior to providing a loan to the MFI. These CIP represent the risk management framework to protect Good Return from the acceptance of MFI partners who

would pose an unacceptable risk to our public reputation and good standing with stakeholders. The procedures for identification and verification of clients are in Appendix A.

2 Customer Identification Procedures (CIP)

The collection of KYC information involves asking the customers to confirm certain pieces of information about their identity and business activities. Verification involves confirming the information provided is correct, based on reliable and independent sources such as primary documents (i.e. articles of association) or electronic sources.

In certain circumstances, additional KYC information must be collected from customers, also known as enhanced customer due diligence (ECDD). This typically applies to customers and/or products and activities that represent a higher ML/TF risk.

Chapter 4 of the AML&CTF Rules refer to the following entity types:

- Individual (chapter 4.2 of the rules)
- Companies (chapter 4.3 of the rules)
- Customers who act in the capacity of trustee of a trust (ch 4.4 of the rules)
- Customers who act in the capacity of member of a partnership (ch 4.5 of the rules)
- Incorporated or unincorporated associations (chapter 4.6 of the rules)
- Registered co-operatives (chapter 4.7 of the rules)
- Government bodies (chapter 4.8 of the rules)

However, as noted below our MFI partners use one of the following legal structures:

- Companies
- Registered co-operatives; or
- Incorporated or unincorporated associations.

They do not maintain complex ownership structures.

2.1 Customer Risk

Factors which are considered to determine the ML/TF risk posed by MFI partners include:

2.2 Politically Exposed Persons (PEPs)

PEPs are considered to carry heightened risk of financial crimes. Good Return considers that a PEP relationship can arise in the following situations:

- Where the client is a natural person, who is classified as a PEP
- Where the prospective MFI partner is a private investment vehicle/Trust which is beneficially owned by a PEP; or
- Where a key representative of an MFI (e.g. director or executive) is a PEP.

Good Return does not engage in partnerships with either types of PEP listed above. Our MFI partners use one of the following legal structures:

- Companies
- Registered co-operatives; or
- Incorporated or unincorporated associations

They do not maintain complex ownership structures.

All prospective MFI partners undergo an extensive due diligence process prior to entering into a partnership with Good Return. Generally, there is a pre-existing relationship with the MFI, where Good Return has been involved in providing training, education and capacity building services to the MFI or their clients.. The MFI engagement process includes the following stages:

- Initial contact
- Completion of an application form
- Desk Due Diligence to assess institution against partnership requirements, including identification and checking of the key personnel
- Letter of intent
- Partner visit to conduct Institutional Assessment and Partnership Outcome discussions
- MOU and Partnership Agreement signed by both parties.

The following documents/tools are relevant to assessment of a prospective MFI partner:

- Country Risk Assessment Tool
- Good Return partnership application
- Good Return Due Diligence overview

- Desk Due Diligence report
- Joint Institutional Assessment

2.3 Jurisdictional Risk

Jurisdictional risk focuses on where the customer, product/service or business is located. Certain countries are known for weak policing of large scale criminal activity or extensive corruption and bribery. Therefore, customers or businesses domiciled in such countries are more likely to pose a higher ML/TF risk particularly if this includes political exposure or entities which are not regulated or supervised. Good Return Program Manual outlines the factors involved in considering the jurisdiction in which a prospective MFI is based. This is considered as part of the Country Risk Assessment.

2.4 Enhanced Customer Due Diligence (ECDD)

ECDD is a risk management process which involves identifying the various potential risk variables posed by clients and balancing out the risks to obtain a comprehensive picture of the actual risk involved. This may involve application of more stringent CDD requirements; escalation and/or additional reputational screening.

Examples of what constitutes ECDD include:

- Asking the MFI partner to provide more information or documentation to mitigate the particular risk identified (e.g. jurisdictional, or where the partner is a charity/religious foundation)
- Performing additional media searches to identify the extent and veracity of any potential reputational risks posed by the client
- Obtaining external due diligence reports to resolve a particular matter (e.g. serious allegations of corruption or wrongdoing).

In the case of customers who are deemed to pose a higher ML/TF risk, we are required to conduct enhanced customer due diligence. For instance, charities or religious foundations have been misused for money laundering and terrorist financing purposes. ECDD would involve verifying that it is duly registered as a legitimate charity.

2.5 Verification of KYC information

The purpose of verification is to provide reasonable and appropriate assurance that the customer's identity has been established. This involves checking the information against reliable and independent sources which can be documentary and/or electronic. The verification procedures are contained in Appendix A.

2.6 Ongoing Customer Due Diligence (OCDD)

Good Return must monitor its MFI partners in relation to the provision of designated services. This section covers its obligation to monitor customers and their transactions on an ongoing basis. OCDD requires Good Return to monitor its customers with a view to identifying, mitigating and managing any ML/TF risk that may be posed by providing the designated services.

AML&CTF Rules specify three mandatory components of OCDD:

- KYC information (ongoing KYC reviews)
- A transaction monitoring program
- An enhanced OCDD program.

Enhanced Customer Due Diligence program is described above.

The Program Manual covers ongoing partnership management. Monitoring and reviews of MFI partners are covered by relevant sections in the Program Manual. At least annually, Good Return staff visit a random sample of the MFI's borrowers to confirm their status. Partnership reviews occur at least annually and include reviewing partnership progress, monitoring a random sample of clients and revising the Partnership Outcome Plan. Good Return staff also conduct periodic in-country spot checks of the MFI's financial management systems.

OCDD involves:

- Reviewing and refreshing existing KYC information with a view to enable us to be satisfied that we still fully understand the MFI partner, including details of its key personnel, throughout the life of the relationship

- Reviewing and assessing the activity of our clients within the relationship to ensure their activity is consistent and reasonable based on our knowledge of the MFI partner.

Therefore Good Return must:

- Collect further KYC information about customers where appropriate and assess whether the ML/TF risk posed by the client has changed in any material way
- Establish and maintain a monitoring program to identify any transaction activity that appears to be suspicious.

The following documents/tools are relevant to the ongoing due diligence on MFI partners:

- Partner Status Review
- Project Progress Report;
- Partner/Field Office Financial Monitoring Report
- Project Monitoring Report
- Financial Monitoring Checklist

2.7 Ongoing KYC reviews

Ongoing KYC reviews are undertaken during annual field audits and client visits. They focus on:

Client KYC Information: fresh validation of KYC information and documentation as needed

AML and Reputational Risk: confirm whether any new AML or Reputational Risk has arisen

Additionally, the various listings of terrorist organisations / sanctioned individuals / ineligible personnel are regularly scanned for mention of our partners or their key personnel.

2.8 Transaction Monitoring Program

The purpose of Good Return's transaction monitoring program is to identify transaction activity that appears to be potentially suspicious. Transaction monitoring is a three-step process:

- Monitor all transactions with the MFI
- Identify suspicious transactions (within the terms of section 41 of the AML&CTF Act)
- Take appropriate action.

A transaction with a MFI may be suspicious if it involves:

- An unusually large size relative to the MFI profile or usual behaviour;
- Changes in loan amounts inconsistent with the size of past average amounts
- There is a significant and unexplained increase in the loan amounts requested or remitted

The Operations manual outlines the processes required to transfer funds to the MFI. It also sets funding limits for MFIs. The Manual contains the periodic tasks required and the required performance standards.

Specific processes in relevant manuals concern the review and approval of payments to MFI partners, payment via Western Union Business Services and reconciliations. The manual covers compliance with legislation and regulations relevant to its operations, including AML&CTF requirements.

3 Reporting Obligations

Where suspicious activity is identified it should be immediately reported to the Financial Controller, or in his absence the CEO. Good Return's reporting obligations under AML&CTF rules include:

- Suspicious matter reporting; and
- Threshold transaction reporting.

3.1 Suspicious Matter Reports (SMRs)

The following matters may give rise to a suspicion under the AML&CTF Act:

- Doubt about identity
- That the MFI's source of funds may be from the proceeds of criminal activity
- Suspicion of financing of terrorism offences
- Suspicion of money laundering offences.
- If required, Financial Controller will lodge a Suspicious Matter Report (SMR) with AUSTRAC.

3.2 Knowledge and Suspicion

Knowledge is regarded as things that Good Return (including Good Return staff) knows, as well as those things that Good Return should have known had we asked obvious questions of other staff, the customer or other third parties.

Suspicion is regarded as more than just mere speculation and being something which requires some foundation, even though this may fall short of belief. However, it should be emphasised, that Good Return is not required to obtain definitive 'proof of guilt' of the underlying offence to report suspicion.

3.3 Unusual Activity

Any member of staff who identifies unusual or suspicious activity must notify the AML&CTF Compliance Officer or in their absence the CEO. Failure to complete the notification is a disciplinary matter that may lead to dismissal. If a staff member makes an unusual activity notification they must not disclose this information to third parties unless authorised by the AML&CTF Compliance Officer.

Further information and analysis must be completed as quickly as the circumstances of the activity notified permits and an assessment is made. All SMRs are to be lodged to AUSTRAC within 3 business days of forming a suspicion unless the suspicion relates to the financing of terrorism in which case an SMR will be lodged within 24 hours of forming a suspicion. The AML&CTF Compliance Officer is responsible for ensuring SMRs are lodged within these required timeframes.

3.4 Threshold Transactions

Where any single transaction of a movement of assets to any MFI partner involves AU\$10,000 or more (or the equivalent of AU\$10,000 or more in another currency) in cash or bitcoin (i.e. physical currency), it must be reported to AUSTRAC within 10 business days. Threshold transaction reports must contain all relevant details of the customer and transaction in accordance with the Rules.

Good Return does not make transactions in cash or bitcoin. Instead, we instruct our banking provider to make the transfer. The bank then has the obligation to make any such TTR.

3.5 Responding to AUSTRAC feedback

Any contact from AUSTRAC is to be referred to the CEO or AML officer for response.

Appendix A Identification and Verification

It is generally fairly straightforward to identify and verify an individual² or a domestic or foreign corporation³. However, identification and verification of unincorporated association, cooperatives, charities, trustee entities and others who may not hold standard identification documents may be more problematic. The following table contains some information that can assist to identify and verify these organisations and individuals.

The following table contains the verification requirements for MFI partners.

Table 1: Identification & Verification Documents:

Entity	Identification & Verification Source Document
Individual	Verify: the name the person via the standard 100 point check adopted by financial institutions & outlined in table 2 in this section.
Corporation	Verify: the full name of the corporation via: An ASIC search or a certified copy of the ASIC certificate of registration, or A search of the relevant market or exchange (e.g. ASX) for a public company or via a search of the relevant State or territory regulator (e.g. APRA for an ADI or Credit Union) or A certified public document issued by the company (e.g. audited annual accounts) or a certificate of registration or incorporation in the foreign jurisdiction or a search of a foreign exchange in the case of a foreign corporation. In relation to any director of the corporation: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.
Unincorporated Association ⁴	Verify: the full name of the association via: – The original or a certified copy of the constitution or rules, or – Minutes of a meeting of the association. In relation to any member of the association: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.
Cooperative ⁵	Verify: the full name of the cooperative via: – A search of the relevant registration body, an original or certified copy of the registration certificate from the relevant state registration body or – An original or certified copy of a register maintained by the cooperative or minutes of its meetings. In relation to the Chairman, Secretary, Treasurer or equivalent officer of the cooperative: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.
Trusts ⁶	Verify: the full name of the trust, trustee/s and beneficiaries via: – An original or certified extract of the trust deed where the name of each is evident or – A letter from a solicitor or qualified accountant that confirms the name of the trust, its trustee/s and beneficiaries.

² Via the standard 100 point check adopted by financial intuitions & discussed later in this section.

³ Via an ASIC search or a certified copy of the ASIC certificate of registration, a search of the relevant market or exchange (e.g. ASX) for a public company or via a search of the relevant State or territory regulator (e.g. APRA for an ADI or Credit Union) or a certified public document issued by the company (e.g. audited annual accounts) or a certificate of registration or incorporation in the foreign jurisdiction or a search of a foreign exchange in the case of a foreign corporation.

⁴ A group of persons who have agreed to join together in pursuit of one or more common objectives, which is not incorporated

⁵ A legal entity owned and controlled by the people for whom it was established and who benefit from using its services. Cooperatives may be registered by a relevant state, territory or overseas body.

⁶ A relationship exists where the trustee holds property or assets for the benefit of the beneficiary or beneficiaries. The trustee may be a corporate trustee or individual trustee/s. There may be more than one trustee or beneficiary.

Where the trustees are individuals: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.
Where the trustee is a corporate trustee it can be identified & verified as for a corporation.

Charities

Verify: the full name of the Charity via:

- A certified copy of the charity's DGR certificate;
- Checking whether the charity has an authority to fundraise by checking with the relevant Office of Charities.⁷

In relation to the chief officers and decisions makers of the charity: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.

Statutory Corporations

Verify: the name of the Statutory Corporation via a copy of the legislation or statutory instrument under which the entity is established.

In relation to the chief officers and decisions makers of the statutory corporation: verify their full name, residential address and date of birth via the verification requirements for individuals, as outlined below.

Individuals who may not hold standard identification documents

Verify: the individuals full name, residential address and date of birth via:

- An indigenous community ID card; or
- A verification form signed by two people who are recognised as leaders or elders of the community to which the individual belongs.

Verification requirements for individuals as mentioned above are two documents from Tables 2A & 2B below and at least one must come from Table 2 A:

Table 2: Verification Requirements

Table 2 A

(At least one of two docs must come from this table)

- Full Birth Certificate – either Australian or foreign*
- Citizenship certificate -either Australian or foreign.
- Passport – either Australian or foreign*
- Australian Drivers' licence or Learner Drivers' licence*
- Pension card – issued by Centrelink or the Department of Veterans Affairs
- Foreign National Identity card*
- Australian Taxi or Boat Licence*

** must contain a photograph and signature*

Table 2 B

- Foreign Drivers' licence*;
- Health Care card - issued by Centrelink or the Department of Veterans Affairs;
- Australian marriage certificate;
- Medicare card;
- Commonwealth Seniors health card or State seniors card;
- Student ID card – Australian Higher Education (TAFE or University)*;
- Security guards licence or Shooters Firearms Licence*;
- Blind Citizens Australia ID card*;
- Multiple Sclerosis Society photo ID card*;
- Australian Public Service Employees card*;
- Working with Children Check card (Blue Card) QLD, Vic & WA*;
- ATO notice issued within the last 12 months including the customer's name & residential address;
- An Australian Financial Institution passbook which is current & has a black light signature;
- Financial Benefits notice issued by a Commonwealth, State or Territory government in the last 12 months including the customer's name & residential address (e.g. a notice from Centrelink);
- Utilities notice issued by a local government or utilities provider within the last 3 months & includes the customer's name & residential address.

Certifying documents:

In Australia: **Certified copy** means a document that has been certified as a true copy of an original document by one of the following persons:

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

⁷ for NSW: <http://wwwdb.dgr.nsw.gov.au/scripts/cfq.exe/notes#history>

- a chief executive officer of a Commonwealth court;
- a registrar or deputy registrar of a court;
- a Justice of the Peace;
- a notary public (for the purposes of the Statutory Declaration Regulations 1993);
- a police officer;
- an agent of the Australian Postal Corporation who is in charge of an office supplying postal services to the public;
- a permanent employee of the Australian Postal Corporation with 2 or more years of continuous service who is employed in an office supplying postal services to the public;
- an Australian consular officer or an Australian diplomatic officer (within the meaning of the Consular Fees Act 1955);
- an officer with 2 or more continuous years of service with one or more financial institutions (for the purposes of the Statutory Declaration Regulations 1993);
- a finance company officer with 2 or more continuous years of service with one or more finance companies (for the purposes of the Statutory Declaration Regulations 1993);
- an officer with, or authorised representative of, a holder of an Australian financial services licence, having 2 or more continuous years of service with one or more licensees;
- a member of the Institute of Chartered Accountants in Australia, CPA Australia or the National Institute of Accountants with 2 or more years of continuous membership.

certified extract means an extract that has been certified as a true copy of some of the information contained in a complete original document by one of the persons described in paragraphs (1)(15).

Offshore certification

In the case of documents from jurisdictions outside Australia Good Return will accept certification completed by the international equivalent of a person listed above. The following registry forums provide information concerning foreign registration bodies:

Registry Forum	Link	Description
Corporate Registers Forum	http://www.corporateregistersforum.org/	The Corporate Registers Forum mainly relates to the Asia-Pacific region, however, it also has the larger American players (US and Canada on-board).
European Commerce Register's Forum	http://www.ecrforum.org/	The European Commerce Register's Forum (ECRF) is made up of 25+ jurisdictions in Europe. It is more business-based, as opposed to solely corporate-form registrations.
International Association of Commerce Administrators	http://www.iaca.org/	The International Association of Commercial Administrators (IACA) is an American association for government administrators of business entity and secured transaction record systems at the state, provincial and national level in any jurisdiction which has or anticipates development of such systems.