AML/CFT PROGRAM MANUAL

AAA MONEY TRANSFER PTY LTD - AML/CTF PROGRAM, V1.0

AAA MONEY TRANSFER PTY LTD

Prepared for	AAA Money Transfer Pty Ltd
Created by	John Waters
Country	Australia
Industry Group	Financial Services
Industry	Money Service Businesses and Money Remitters

GENERAL INFORMATION

About this document

This document forms part of the AML Program Manual provided by AML Accelerate, which has been designed to address and comply with the relevant AML/CFT legal and regulatory obligations.

This document should be read in conjunction with the other related documents, which form components of the AML Program Manual:

- **Company Information -** which contains contextual information relating to our organisation;
- **ML/TF Risk Assessment -** which contains the outputs of a structured process of identifying, assessing ML/TF risks and the controls in place to manage and mitigate the ML/TF risk an organisation may reasonably face;
- **AML Program -** which contains the approach to addressing the relevant AML/CFT legal and regulatory requirements for a type of business;
- **Customer Due Diligence Standards -** which contains the type and extent of due diligence undertaken on customers, based on their legal form and their assessed level of ML/TF risk; and
- **Appendices -** which contains a glossary of key terms, a list of reference materials used in the preparation of the AML/CFT Program Manual, and other supporting information and documents.

The AML Accelerate platform also provides the ability to create a supporting AML operating manual. Where an AML operating manual has been created, it should be read in conjunction with the documents contained within the AML Program Manual.

Disclaimer

By using the AML Accelerate platform, you have agreed to Financial Crimes Consulting Pty Ltd's terms of use and, if applicable, the end user licence agreement. Prior to publishing the results or making use of the AML Accelerate platform or any of the component documents ("Materials"), it is strongly recommended that such Materials are reviewed by your professional advisers to ensure they are appropriately tailored to your organisation's specific situation and requirements. The AML Accelerate platform and the Materials contain statements of opinion as at the date on which they are made, and do not constitute statements of fact or amount to any legal or other professional advice.

In deciding to make use of the AML Accelerate platform, you are not relying on the accuracy, reliability or factual correctness of the AML Accelerate platform or the Materials. Financial Crimes Consulting Pty Ltd accepts no liability, and provides no warranties, as to the applicability of the AML Accelerate platform or the Materials to your organisation's specific circumstances or any loss that you suffer as a result of you making use of the AML Accelerate platform or the Materials. You make use of the AML Accelerate platform and the materials at your own risk and in your sole and absolute discretion.

Table of Contents

1 Company Information

1.1 General

Registration Information

Legal Status	Company/Corporation
Legal Name	AAA Money Transfer Pty Ltd
Country of Incorporation/Registration	Australia
Date of Incorporation/Registration	23-Jan-2015
Name of Registration Body	ASIC
Registered Business Number	ACN 603 845 272

1.2 Address Details

Registered Office Address

Address Line 1	1330 Malvern Road
City, Town or Suburb	Malvern
State/County	VIC
Postcode	3144
Country	Australia

Principal Place of Business Address

Address Line 1	10 McCrae Street
City, Town or Suburb	Dandenong
State/County	VIC
Postcode	3175
Country	Australia

1.3 Business Profile

Nature, Size and Complexity of the Business

Context	We are a small money transfer business servicing our local community. We utilise the following remittance network providers; Western Union, and Ria.
Annual Revenue (in local currency)	AUD$ 1,000,001-5,000,000

Approximate Number of Customers	501-1,000
Number of outlets/branches or offices	01
Number of Employees	1-25
Are you part of a group or a subsidiary of another entity?	No
Attachment(s) e.g. organisational chart	Western Union - Global Fraud Policy and Procedure.pdf

1.4 AML Compliance Officer

Name and Contact Details of AML Compliance Officer

Full Name	Duy Su Nguyen
Position/Title	Manager
Address Line 1	10 McCrae Street
City, Town or Suburb	Dandenong
State/County	State
Postcode	3175
Country	Australia
Mobile	0423 969 535
E-mail	derrickng08@yahoo.com.au

Alternate Contact Person Details

Full Name	Anna Nguyen
Position/Title	Director
Mobile	0435 541 988
E-mail	annan_2008@hotmail.com

1.5 Regulatory Information

Name of AML/CFT Regulator	AUSTRAC

2 ML/TF Risk Assessment

2.1 Executive Summary

This section provides an overall summary of the ML/TF risk assesment that was conducted by AAA Money Transfer Pty Ltd.

Context
We are a small money transfer business servicing our local community. We utilise the following remittance network providers;
Western Union, and
Ria.

Overall ML/TF Risk Rating
An ML/TF risk assessment has been conducted with inputs from different risk factors and the table below summarises the overall ML/TF Risk Rating based on the aggregate Residual Risk:

Overall ML/TF Risk Rating	**Low**

Comments
No comments provided.

2.2 Risk Categories

This section provides an overall summary of the ML/TF risk assessment conducted by AAA Money Transfer Pty Ltd.

2.2.1 ML/TF Risk Rating by Risk Category

The overall ML/TF Risk Rating is based on each of the following risk categories.

RISK CATEGORIES	RESIDUAL RISK RATING
Environmental Risk	Low
Customer Risk	Low
Business Risk	Low
Channel Risk	Low
Product Risk	Low

Note: The assessment of country risk is undertaken on a country by country basis only because of its impact on other risk categories. Country risk is incorporated within customer, business and channel risks.

Comments

No comments provided.

2.2.2 Control Summary

The table below summarises the existence of controls at the risk factor level within each risk sub-category and risk category:

RISK CATEGORY	RISK SUB-CATEGORY	RISKS	IRR	CONTROLS ADDED	NOT TESTED	POOR	ADEQUATE	EXCELLENT	RRR
Environmental Risk	Predicate Offence	Deceptive Crimes	L	Yes			9		L
		Illicit Trafficking	L	Yes			9		L
		Personal Crimes	L	Yes			9		L
		Property Crimes	L	Yes			9		L
	Money Laundering	Higher Risk Business Operations	L	Yes			12		L
		Higher Risk Channels	L	Yes			12		L
		Higher Risk Customer Transactions	L	Yes			12		L
		Higher Risk Customers	L	Yes			12		L
		Higher Risk Products and Services	L	Yes			12		L

RISK CATEGORY	RISK SUB-CATEGORY	RISKS	IRR	CONTROLS ADDED	NOT TESTED	POOR	ADEQUATE	EXCELLENT	RRR
	Terrorist Financing	Higher Risk Customer	L	Yes			13		L
		Higher Risk Customer Transactions	L	Yes			13		L
	Targeted Financial Sanctions	Higher Risk Customer	L	Yes			5		L
		Higher Risk Customer Transactions	L	Yes			5		L
	Regulatory Compliance	Governance & Oversight	L	Yes			9		L
		Program Alignment to ML/TF Risks	L	Yes			9		L
		Program Non-Compliance	L	Yes			9		L
		Reporting	L	Yes			9		L
Customer Risk	-	-	L	Yes			7		L
Business Risk	-	-	M	Yes			4		L
Channel Risk	-	-	M	Yes			3		L
Product Risk	-	Remittance - International	M	Yes			7		L
				Total	**0**	**0**	**189**	**0**	

Key

IRR = Inherent Risk Rating	RRR = Residual Risk Rating

L	Low Risk	M	Medium Risk
H	High Risk	S	Significant Risk

Comments

No comments provided.

2.2.3 Environmental Risk

This section guides you through a structured ML/TF Risk Assessment process and has been designed by experts to assist your organisation in identifying, assessing, mitigating and managing money laundering and terrorism financing risk exposures.

2.2.3.1 ML/TF Risk Rating by Risk Sub-Category

The Environmental Risk section of the ML/TF Risk Assessment is based on the following risk sub-categories.

RISK SUB-CATEGORY	RESIDUAL RISK RATING
Predicate Offence	**Low**
Money Laundering	**Low**
Terrorist Financing	**Low**
Targeted Financial Sanctions	**Low**
Regulatory Compliance	**Low**

In each of the sections below the report provides the further information on how the risk score was calculated.

Comments

No comments provided.

2.2.3.2 Predicate Offence

ML/TF Risk Rating by Individual Risk

The overall ML/TF Risk Rating is based on each of the following risks.

RISK	INHERENT RISK RATING	RESIDUAL RISK RATING
Deceptive Crimes	Low	Low
Illicit Trafficking	Low	Low
Personal Crimes	Low	Low
Property Crimes	Low	Low

Comments
No comments provided.

2.2.3.2.1 Deceptive Crimes

Deceptive crimes are offences when someone intentionally deceives someone to dishonestly benefit or to cause a detriment to someone. The deception can be done by words or conduct and deceptive crimes include, bribery and corruption, counterfeit goods and currency, forgery, fraud, insider trading, market manipulation, and tax crimes/tax evasion.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	No	Yes	Yes	No	Yes	Yes

Risk Indicator(s)

- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services
- Customers hold positions that may make them vulnerable to corruption, such as being a politically exposed person (PEP)
- Customers from countries that have been identified as vulnerable to corruption
- Funds to/from countries that have been identified as vulnerable to deceptive crimes such as counterfeit goods, bribery and corruption, or tax evasion

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Deceptive Crimes Inherent Risk Rating — Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.

Rationale/Additional Comments
No rationale/additional comments provided.

Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/ TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Deceptive Crimes Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.2.2 Illicit Trafficking

Illicit trafficking is the illegal trading, selling or dealing in specified goods, such as arms and weapons; drugs; humans and human body parts, as well as some environmental crimes, such as illegal logging/fishing and the trade in endangered animals and their body parts. Illicit trafficking also includes smuggling.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	No	Yes	Yes	No	Yes	Yes

Risk Indicator(s)

- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services
- Customers from countries that have been identified as vulnerable to illict trafficking crimes
- Funds to/from countries that have been identified as vulnerable to illict trafficking crimes

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Illicit Trafficking Inherent Risk Rating	Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.

Rationale/Additional Comments

No rationale/additional comments provided.

Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Illicit Trafficking Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.2.3 Personal Crimes

Personal crimes are violent crimes in which an offender uses or threatens force upon a victim. This entails both crimes in which the violent act is the objective, such as murder, as well as crimes in which violence is the means to an end. Violent crimes may, or may not, be committed with weapons. Personal crimes can also include kidnap, illegal restraint and hostage taking, and sexual exploitation.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	No	Yes	Yes	No	Yes	Yes

Risk Indicator(s)

- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services
- Customers from countries that have been identified as vulnerable to personal crimes such as kidnap, hostage taking or sexual exploitation
- Funds to/from countries that have been identified as vulnerable to personal crimes such as kidnap, hostage taking or sexual exploitation

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	**If the risk were to occur what impact would it have on your business?**	Moderate

Personal Crimes Inherent Risk Rating	**Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.

Rationale/Additional Comments

No rationale/additional comments provided.

Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Personal Crimes Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.2.4 Property Crimes

Property crime is a crime to obtain money, property, or some other benefit, this may involve force, or the threat of force. Property crime is a category of crime that includes, burglary, theft, robbery, extortion, and the trafficking in stolen goods.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	No	Yes	Yes	No	Yes	Yes

Risk Indicator(s)

- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Property Crimes Inherent Risk Rating	Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

Rationale/Additional Comments

No rationale/additional comments provided.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Property Crimes Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.3 Money Laundering

ML/TF Risk Rating by Individual Risk

The overall ML/TF Risk Rating is based on each of the following risks.

RISK	INHERENT RISK RATING	RESIDUAL RISK RATING
Higher Risk Business Operations	Low	Low
Higher Risk Channels	Low	Low
Higher Risk Customer Transactions	Low	Low
Higher Risk Customers	Low	Low
Higher Risk Products and Services	Low	Low

Comments

No comments provided.

2.2.3.3.1 Higher Risk Business Operations

Business operations could involve higher money laundering risk jurisdictions, or employees could collude with a customer to facilitate or allow money laundering by the customer using your products and services.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	No	Yes	Yes	No	No

Risk Indicator(s)

- Third parties undertake business operations and/or AML/CFT controls
- Business operations or third parties used to operate AML/CFT controls are located in high money laundering risk countries
- Employees unusually close to, or protective of, particular customer relationships

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business? Unlikely

If the risk were to occur what impact would it have on your business? Moderate

Higher Risk Business Operations Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.

Rationale/Additional Comments

No rationale/additional comments provided.

Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Business Operations Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.3.2 Higher Risk Channels

Channels used to deliver products to customers or customers are engaged in a way that could facilitate the remote or anonymous use of products and accounts.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	Yes	Yes

Risk Indicator(s)

- Business is conducted with customers on a non face-to-face basis
- Business is conducted using third parties to engage with customers and deliver your products/services
- Third parties used to attract/engage with customers and deliver your products/services are located in high money laundering risk countries

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Higher Risk Channels Inherent Risk Rating — **Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.

Rationale/Additional Comments

No rationale/additional comments provided.

Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Channels Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.3.3 Higher Risk Customer Transactions

Transactions undertaken by a customer or group of connected customers could be for the purpose of laundering money or facilitating/supporting a predicate offence.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	Yes	Yes

Risk Indicator(s)

- Customers making large overseas transactions with no apparent valid or available explanation or documentation
- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business? Unlikely

If the risk were to occur what impact would it have on your business? Moderate

Higher Risk Customer Transactions Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.

Rationale/Additional Comments

No rationale/additional comments provided.

Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customer Transactions Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.3.4 Higher Risk Customers

Customers using your products and services, could be a higher money laundering risk due to an inability to identify them, the business activities they undertake, their location or status (PEP).

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	No	No

Risk Indicator(s)

- Customers that are unable or unwilling to have their identity established and/or verified
- Customers are defined high money laundering risk customer types
- Customers are from high money laundering risk countries

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Higher Risk Customers Inherent Risk Rating — **Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.

Rationale/Additional Comments

No rationale/additional comments provided.

Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customers Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.3.5 Higher Risk Products and Services

Products and services offered could facilitate money laundering by breaking the audit trail and moving money between asset classes and between different jurisdictions.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	No	No	No	No	Yes

Risk Indicator(s)

- Products are very flexible and support the conversion of assets from one type to another
- Products facilitate overseas payments or transactions
- Products that allow the receipt or payment of cash
- Products that support the concealment ownership and control of assets or funds

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Higher Risk Products and Services Inherent Risk Rating — **Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk	Rationale/Additional Comments
AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.	*No rationale/additional comments provided.*
AML Training - AML training provided to all staff.	
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.	
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.	
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.	
Employee Due Diligence - Identity, police and referee checks on employees.	
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.	
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.	

Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Products and Services Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.4 Terrorist Financing

ML/TF Risk Rating by Individual Risk

The overall ML/TF Risk Rating is based on each of the following risks.

RISK	INHERENT RISK RATING	RESIDUAL RISK RATING
Higher Risk Customer	Low	Low
Higher Risk Customer Transactions	Low	Low

Comments

No comments provided.

2.2.3.4.1 Higher Risk Customer

Customer could be associated with terrorism or terrorist financing, or the countries they are located in are higher terrorist financing or terrorist risk jurisdictions.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	No	No

Risk Indicator(s)

- Customer is on the United Nations Terrorist list or other relevant sanction list
- Customers that are unable or unwilling to have their identity established and/or verified
- Customers are defined high terrorism or terrorist financing risk customer types, such as charities and charitable foundations
- Customers are from high terrorism or terrorist financing risk countries

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Higher Risk Customer Inherent Risk Rating	Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.

Rationale/Additional Comments

No rationale/additional comments provided.

Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.
Transaction Screening - Sanction list screening of transactions, including remitters and beneficiaries of transactions.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customer Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.4.2 Higher Risk Customer Transactions

Customer transactions could be associated with the planning, preparation commission or execution of terrorist acts or the financing of terrorism.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	Yes	Yes

Risk Indicator(s)

- The name of the sender, beneficiary or intermediary entity of a customer transaction is on the United Nations Terrorist list or other relevant sanction list
- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business? Unlikely

If the risk were to occur what impact would it have on your business? Moderate

Higher Risk Customer Transactions Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Employee Due Diligence - Identity, police and referee checks on employees.
Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.

Rationale/Additional Comments

No rationale/additional comments provided.

Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.
Transaction Screening - Sanction list screening of transactions, including remitters and beneficiaries of transactions.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customer Transactions Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.5 Targeted Financial Sanctions

ML/TF Risk Rating by Individual Risk

The overall ML/TF Risk Rating is based on each of the following risks.

RISK	INHERENT RISK RATING	RESIDUAL RISK RATING
Higher Risk Customer	Low	Low
Higher Risk Customer Transactions	Low	Low

Comments

No comments provided.

2.2.3.5.1 Higher Risk Customer

Customers could be Special Designated Nationals and subject to targeted financial sanctions against persons and entities.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	Yes	No	No	No	No

Risk Indicator(s)

- Customers that are unable or unwilling to have their identity established and/or verified
- Customers are from countries who have people and/or entities subject to targeted financial sanctions
- Name of the customer appears on the relevant sanction lists

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business? Unlikely

If the risk were to occur what impact would it have on your business? Moderate

Higher Risk Customer Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.

Rationale/Additional Comments

No rationale/additional comments provided.

Transaction Screening - Sanction list screening of transactions, including remitters and beneficiaries of transactions.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customer Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.5.2 Higher Risk Customer Transactions

Transactions involve persons and entities subject to sanction, or transactions undertaken may breach sanctions that prohibit the supply of particular goods and services.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
Yes	Yes	No	No	No	Yes	Yes

Risk Indicator(s)

- The transaction involves or is related to the provision of goods or services that are designated/prohibited by the sanction regimes relevant to your organisation
- Customers that are unable or unwilling to explain the source of the funds or assets associated with the use of your products or services
- Customers that exhibit behaviour that is unusual with reference to the type of customer and the usual use of your products or services
- The name of the sender, beneficiary or intermediary entity appears on the relevant sanction lists

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business? Unlikely

If the risk were to occur what impact would it have on your business? Moderate

Higher Risk Customer Transactions Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Transaction Screening - Sanction list screening of transactions, including remitters and beneficiaries of transactions.

Rationale/Additional Comments
No rationale/additional comments provided.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Higher Risk Customer Transactions Residual Risk Rating Low

Comments
No comments provided.

2.2.3.6 Regulatory Compliance

ML/TF Risk Rating by Individual Risk

The overall ML/TF Risk Rating is based on each of the following risks.

RISK	INHERENT RISK RATING	RESIDUAL RISK RATING
Governance & Oversight	Low	Low
Program Alignment to ML/TF Risks	Low	Low
Program Non-Compliance	Low	Low
Reporting	Low	Low

Comments

No comments provided.

2.2.3.6.1 Governance & Oversight

The appropriate oversight and governance arrangements are not in place to ensure your AML Program is effective.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
No	Yes	No	Yes	No	No	No

Risk Indicator(s)

- Your organisation has not appointed a AML Compliance Officer or the AML Compliance Officer does not have the appropriate skills or experience
- Your organisation has not adequately resourced its AML/CFT compliance function
- Your organisation is not conducting appropriate internal oversight to check the level of AML/CFT compliance and the effectiveness of AML/CFT controls
- Your organisation is not commissioning independent reviews or external audits, required by relevant law and regulation
- Your organisation is not commissioning independent reviews or external audit with the appropriate frequency and scope
- Your organisation has not put in place appropriate processes to approval your AML Program, or governance around developing/ changing the AML Program

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Governance & Oversight Inherent Risk Rating — Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.

Rationale/Additional Comments

No rationale/additional comments provided.

Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Senior Management/Board Oversight - Periodic or routine oversight by the most senior management of your organisation to ensure AML/CFT compliance and the effectiveness of AML/CFT controls.
Calendar of Activities - Calendar setting out all the AML compliance activities for a calendar year.
Independent Review - Requirement to have an external review of the AML Program to ensure compliance with AML rules and laws.
Regulator Feedback - Process for receiving and responding to feedback from regulators.
Reporting Entity Registration - Meeting the registration obligation and then ensuring that regulators are informed of changes in business profile.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Governance & Oversight Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.6.2 Program Alignment to ML/TF Risks

Your organisation does not understand the ML/TF risks it faces, or AML/CFT Program does not address the ML/TF risk faced, resulting from customers, business operations, the channels used to engage customers, or products and services offered.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
No	Yes	No	Yes	No	No	No

Risk Indicator(s)

- Your organisation has no ML/TF Risk Assessment in place
- The ML/TF Risk Assessment does not cover all relevant ML/TF risks for your organisation
- The ML/TF Risk Assessment does not adequately assess all relevant ML/TF risks for your organisation
- The ML/TF Risk Assessment is not updated periodically, or when events or triggers occur within your business that mean the ML/TF risks may have changed

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	If the risk were to occur what impact would it have on your business?	Moderate

Program Alignment to ML/TF Risks Inherent Risk Rating	Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk
AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Senior Management/Board Oversight - Periodic or routine oversight by the most senior management of your organisation to ensure AML/CFT compliance and the effectiveness of AML/CFT controls.
Calendar of Activities - Calendar setting out all the AML compliance activities for a calendar year.
Independent Review - Requirement to have an external review of the AML Program to ensure compliance with AML rules and laws.
Regulator Feedback - Process for receiving and responding to feedback from regulators.
Reporting Entity Registration - Meeting the registration obligation and then ensuring that regulators are informed of changes in business profile.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.

Rationale/Additional Comments

No rationale/additional comments provided.

Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Program Alignment to ML/TF Risks Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.6.3 Program Non-Compliance

The business arrangements, systems and controls put in place are non-compliant with the relevant AML/CFT laws and regulation, or not following the requirements and controls set out in your AML/CFT Program.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
No	Yes	Yes	Yes	No	Yes	Yes

Risk Indicator(s)

- Your organisation's AML Program does not cover all the AML/CFT obligations set out in the relevant AML/CFT law and regulations
- Your organisation's AML Program does not adequately address obligations set out in the relevant AML/CFT law and regulations
- Your organisation has not adequately implemented the controls set out in your AML Program
- Inadequate resources have been made available to implement or operate your AML Program
- Your organisation and/or the businesses are not effectively operating the controls set out in your AML Program

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	**If the risk were to occur what impact would it have on your business?**	Moderate

Program Non-Compliance Inherent Risk Rating — **Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Senior Management/Board Oversight - Periodic or routine oversight by the most senior management of your organisation to ensure AML/CFT compliance and the effectiveness of AML/CFT controls.
Calendar of Activities - Calendar setting out all the AML compliance activities for a calendar year.
Independent Review - Requirement to have an external review of the AML Program to ensure compliance with AML rules and laws.
Regulator Feedback - Process for receiving and responding to feedback from regulators.
Reporting Entity Registration - Meeting the registration obligation and then ensuring that regulators are informed of changes in business profile.

Rationale/Additional Comments

No rationale/additional comments provided.

Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Program Non-Compliance Residual Risk Rating **Low**

Comments
No comments provided.

2.2.3.6.4 Reporting

Not completing the required reporting required by relevant law and regulation, which may include cash transactions over a defined threshold, suspicious activity or matters identified, and levels compliance with AML/CFT requirements by your organisation.

Risk Applicability

BUSINESS RISK	CHANNEL RISK	CUSTOMER RISK	EMPLOYEE RISK	EXTERNAL RISK	INTERNAL RISK	PRODUCT RISK
No	Yes	No	Yes	No	No	No

Risk Indicator(s)

- Your organisation is not able to collate/collect the information and data necessary to complete reporting requirements
- Your organisation is not filing threshold transaction or other transaction reports required by AML/CFT law and regulation
- Your organisation is not filing suspicious matter, suspicious transaction, or suspicious activity, reports required by AML/CFT law and regulation
- Your organisation is not filing compliance reports required by AML/CFT law and regulation

INHERENT RISK RATING

How likely is it that the risk indicators could occur in your business?	Unlikely	**If the risk were to occur what impact would it have on your business?**	Moderate

Reporting Inherent Risk Rating — **Low**

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Senior Management/Board Oversight - Periodic or routine oversight by the most senior management of your organisation to ensure AML/CFT compliance and the effectiveness of AML/CFT controls.
Calendar of Activities - Calendar setting out all the AML compliance activities for a calendar year.
Independent Review - Requirement to have an external review of the AML Program to ensure compliance with AML rules and laws.
Regulator Feedback - Process for receiving and responding to feedback from regulators.
Reporting Entity Registration - Meeting the registration obligation and then ensuring that regulators are informed of changes in business profile.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.

Rationale/Additional Comments

No rationale/additional comments provided.

Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Reporting Residual Risk Rating **Low**

Comments
No comments provided.

2.2.4 Customer Risk

LOCATION RISK ASSESSMENT

Are all of your customers based in the same country as your registered business address?
Yes

Customer Location Risk Low

BUSINESS RISK ASSESSMENT

Do your customers undertake any of the following higher ML/TF risk business activities?

Accounting Professionals	2%
Percentage of customers that are engaged in higher ML/TF risk business activities	**2%**

Customer Business Risk Low

Customer Footprint Risk Rating Low

PEP RISK ASSESSMENT

Are any of your customers Politically Exposed Persons?
No

Customer PEP Risk Rating Low

CUSTOMER TYPE RISK ASSESSMENT

Are all your Customers Individuals
Yes

If no, provide the distribution of customers by customer type

	Distribution	Higher Risk
Individual	100%	2%
Percentage of customers by customer type	**100%**	

Customer Legal Form Risk Rating Low

Customer Type Risk Low

Customer Inherent Risk Rating Low

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Customer Due Diligence - The process of accepting customers and verifying their identity as required by AML legal and regulatory requirements.
Customer Screening - List screening of customers, agents and related parties, for sanctions and ML/TF risks such as PEPs and negative media.

Rationale/Additional Comments
No rationale/additional comments provided.

Enhanced Customer Due Diligence - The process of collecting additional information about a customer when ML/TF risk is high.
Ongoing Customer Due Diligence - Refreshing customer and enhanced customer due diligence on a periodic basis or when required to do so.
Record Keeping - Keeping records of transactions, customer identification documents and AML program records.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Customer Residual Risk Rating **Low**

Comments
No comments provided.

2.2.5 Business Risk

BUSINESS LOCATION RISK ASSESSMENT

Are all of your business operations in the same country as your registered business address?
Yes

Business Location Risk Rating Low

OUTSOURCE RISK ASSESSMENT

Do you use third parties as part of AML/CFT controls?
No

Business Outsource Control Risk Rating Low

Business Operations Risk Rating Low

EMPLOYEE RISK ASSESSMENT

What is your total number of employees?
02

How many of your employees have had an adverse employee screening result?
0

Business Employee Screening Risk Rating Low

What percentage of your employees are customer facing?
100%

In which of the following higher ML/TF risk roles does your business employee staff and what functions do they perform?

Role		Functions Performed				
		Customer Services and Support	Maintenance of Customer and Transaction Data	Approval of non-standard facilities and policy overrides	Payment Processing	Developing and Operating the AML/CFT Program
Transaction Processing	100%	Yes	Yes	Yes	Yes	Yes
Percentage of employees that occupy higher risk roles	**100%**					

Business Employee Role Risk Rating High

Business Employee Risk Rating Medium

Business Inherent Risk Rating Medium

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.

Rationale/Additional Comments
No rationale/additional comments provided.

Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.
Employee Due Diligence - Identity, police and referee checks on employees.
Reporting Entity Registration - Meeting the registration obligation and then ensuring that regulators are informed of changes in business profile.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Business Residual Risk Rating **Low**

Comments
No comments provided.

2.2.6 Channel Risk

NON - FACE TO FACE RISK ASSESSMENT

Do you meet all of your customers face to face?
Yes

Which of the following methods do you use to interact with your customers? (please select all that apply)
Branch Network

Channel Non-Face To Face Risk Rating — Low

THIRD PARTY USE RISK ASSESSMENT

Does your business use third parties to sell products or engage with customers?
Yes

If yes, what percentage of your customers are engaged through a third party?
100%

Are all the third parties located in the same country as your registered business address?
No

If no, provide the distribution of third parties that are in overseas countries?

Philippines	95%
Liberia	2%
Sierra Leone	2%
Vietnam	1%
Percentage of third parties that are overseas	**100%**

Channel Third Party Use Risk Rating — High

Channel Third Party Location Risk Rating — High

Channel Third Party Risk Rating — High

Channel Inherent Risk Rating — Medium

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
Assurance Processes - The AML Compliance Officer or Internal Audit function routinely check that procedures (controls) have been carried out correctly.

Rationale/Additional Comments
No rationale/additional comments provided.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Channel Residual Risk Rating — Low

Comments

No comments provided.

2.2.7 Product Risk

Product risk exposure and its distribution across the customer base

PRODUCT	INHERENT RISK RATING	CUSTOMERS	REVENUE	AUTOMATED OR MANUAL MONITORING?	SUSPICIOUS REPORTS	RESIDUAL RISK RATING
Remittance - International	Medium	100.00%	100.00%	Yes	0	Low

Comments
No comments provided.

2.2.7.1 Remittance - International

Electronic transfer of funds across national borders.

- This is a high risk product based on typologies. It provides a way to move funds overseas/internationally.

RISK FACTORS		RISK FACTORS	
Can the product allow funds to be transferred in anonymously?	No	Can the product allow funds to be transferred out anonymously?	No
Can the product allow funds to be deposited in more than one way?	Yes	Can the product allow funds to be withdrawn in more than one way?	No
Can the product allow funds to be deposited by a third party?	No	Can the product allow funds to be withdrawn by a third party?	No
Can the product allow funds to be deposited using remote access?	No	Can the product allow funds to be withdrawn using remote access?	No
Can the product allow funds to be accepted from a foreign jurisdiction?	No	Can the product allow funds to be withdrawn in a foreign jurisdiction?	Yes
Can the product allow or facilitate multiple deposits?	No	Can the product allow or facilitate multiple withdrawals?	No
Can the product allow funds to be held for a non-fixed term?	No	Can the product allow a cooling off period during which funds can be returned?	No
Can the product allow inward transactions of unlimited value?	No	Can the product allow outbound transactions of unlimited value?	No
Can the product allow early or over payment?	No	Can the product allow transactions over the minimum repayment/ premium?	No
Can the product allow cash payments or deposits to be accepted?	Yes	Can the product allow cash withdrawals?	Yes

Remittance - International Inherent Risk Rating Medium

RISK EXPOSURE AND ITS DISTRIBUTION ACROSS THE CUSTOMER BASE

What percentage of your customer base use this product or 100%

service?	
What percentage of your overall annual revenue is attributable to this product?	100%
Do you perform any automated or manual monitoring for this product or service?	Yes
How many reports of suspicion have you made involving this product or service?	0

RESIDUAL RISK RATING

Control(s) that should mitigate risk

AML Program - Documented set of policies and procedures that meet the requirements of the AML rules and laws.
AML Training - AML training provided to all staff.
International Funds Transfer (Wire Transfer) Reporting - Reporting International Funds Transfer Instructions.
Suspicious Activity/Matter Reporting - Procedures to file suspicious activity/matter reports with the AML regulator.
Threshold Transaction Reporting - Reporting cash transactions over the prescribed threshold amount.
Transaction Monitoring - Monitoring all transactions looking for red flags and outliers. Includes regular reports covering same.
Transaction Screening - Sanction list screening of transactions, including remitters and beneficiaries of transactions.

Rationale/Additional Comments
No rationale/additional comments provided.

How effective are the mitigating control(s)?
Adequate

Items
No item(s) linked.

Remittance - International Residual Risk Rating **Low**

Comments
No comments provided.

2.2.8 Country Risk

COUNTRY RISK	COUNT
Restricted	0
High	2
Medium	2
Low	1
Total	**5**

REGION	COUNTRY	DEFAULT RISK RATING	CUSTOM RISK RATING	RATIONALE FOR CUSTOM RATING
Africa	Liberia	High		
Africa	Sierra Leone	Medium		
Asia	Philippines	High		
Asia	Vietnam	Medium		
Oceania	Australia	Low		

Comments
No comments provided.

3 AML Program

3.1 AML/CTF program scope

3.1.1 Program Scope

We are a money remittance business with affiliate relationships with the following remittance network providers:

- Western Union; and
- Ria.

Whilst we operate our business independently and through multiple remittance network providers, we have a single AML/CTF Program for all our business activity.

Where a particular remittance network provider requires additional controls for transaction through them, we will ensure we comply with these additional requirements.

3.1.2 Description of business

We are a reporting entity, because as a money service provider / money remitter, we undertake the following activities defined within chapter 6, table 1 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act).

- Providing remittance services

3.1.3 AML/CTF program coverage

Part 8.1 of the AML/CTF Rules requires that the AML/CTF program applies only to the parts of our business that provide products and services covered by the AML/CTF Act and AML/CTF Rules.

Where our business provides products and services not covered by AML/CTF Act and AML/CTF Rules, those parts of our business are outside the scope of this AML/CTF program.

3.2 AML/CTF program

3.2.1 AML/CTF program objectives

In designing and adopting this AML/CTF program, we aim to:

- Comply with Australia's AML/CTF laws and regulations;
- Make sufficient funding and resources available for the implementation of the AML/CTF program;
- Provide our products and services only for legitimate purposes to customers whose identities we have been able to verify;
- Identify our customers and monitor their transactions to a degree consistent with the level of money laundering and terrorist financing (ML/TF) risk they represent;
- Educate our people about the risks of ML/TF and the behaviours and actions we require of them to make our effective; and
- Manage changes to our products, business processes and systems to ensure that ML/TF risks are identified, managed and mitigated.

Part 8.1 of the AML/CTF Rules sets out that our AML/CTF Program is required to be divided into Parts A and B.

In line with the requirements of Part 8.1 of the AML/CTF Rules, Part A of the AML/CTF program records our approach to the identification, mitigation and management of the ML/TF risks we reasonably face.

Our approach is determined by the AML/CTF Act and AML/CTF Rules, which include:

- Putting in place systems and processes to assess the ML/TF risk of customers, business operations, channels and the products and services we provide;
- Establishing appropriate systems and controls to identify, manage, and mitigate our ML/TF risks;
- Undertaking appropriate oversight of the AML/CTF program and its continued effectiveness at managing and mitigating our ML/TF risks;
- Implementing employee screening and ongoing monitoring of staff;

- Undertaking employee training and education in AML/CTF trends, risk-based processes and the consequences of non-compliance;
- Undertaking training and ongoing monitoring of agents and third parties (if applicable);
- Implementing ongoing customer due diligence (CDD), including enhanced due diligence measures and monitoring of customer transactions;
- Undertaking suspicious matter reporting and other reporting required by AML/CTF Act and AML/CTF Rules;
- Providing for the independent review of Part A of the AML/CTF Program;
- Appointing an AML Compliance Officer;
- Responding to AUSTRAC feedback; and
- Ensuring permanent establishments in a foreign country (if applicable).

Part B of the AML/CTF program relates to customer identification procedures and includes conducting CDD to identifying customers (and their agents) to enable us to be reasonably satisfied that a customer is who they claim to be.

CDD includes:

- Collecting and verifying customer identification information – for example, documents, data or other information obtained from reliable and independent sources;
- Identifying and verifying the beneficial owner(s) of a customer;
- Identifying whether a customer is a politically exposed person (PEP) or an associate of a PEP and taking steps to establish the source of funds used during the business relationship or transaction;
- Undertaking ongoing CDD and transaction monitoring; and
- Obtaining information on the purpose and intended nature of the business relationship.

The AML/CTF program also records our approach to the risk that our business, including the products and services we offer, might be used to breach targeted financial sanctions in place in Australia or relevant countries overseas.

Aspects of these sanction risks are outside of the scope of the AML/CTF Act and AML/CTF Rules, but as the controls are like those required for AML/CTF, we manage them within the AML/CTF program.

3.2.2 AML/CTF program core principles

Through Part A of our AML/CTF program, we have adopted the following core principles for our business:

- We are opposed to the crimes of ML/TF and do not tolerate the use of our products and services for either of these purposes;
- We will ensure that we meet our AML/CTF legal and regulatory obligations and that our employees are trained in their obligations and how to comply with these legal and regulatory obligations;
- We will protect ourselves and our people from the reputation damage, regulatory intervention and financial penalties that could be imposed for non-compliance with AML/CTF obligations;
- We have established and maintained an AML/CTF program that seeks to reasonably identify, mitigate and manage the ML/TF risks we reasonably face;
- Where we detect any suspicious matter or activity that falls within chapter 41 of the AML/CTF Act, we will report this to the AUSTRAC CEO;
- We will monitor our own customers and all requests for transactions in a manner consistent with the level of ML/TF risk they represent; and
- We will work with AUSTRAC to ensure that we meet their expectations.

3.2.3 AML/CTF program approval

This version of Part A of the AML/CTF program has been reviewed and approved by the owner. Evidence of approval by all those required to approve the AML/CTF program has been retained by the AML Compliance Officer.

3.2.4 AML/CTF program adoption

This version of Part A the AML/CTF program is adopted from the date of approval.

3.2.5 AUSTRAC Enrollment

Section 51 of the AML/CTF Act and chapter 8 of the AML/CTF Rules require we enroll with AUSTRAC and advise AUSTRAC of any changes to the information provided on enrollment.

The AML/CTF Compliance Officer is responsible for ensuring we have enrolled with AUSTRAC and maintain enrollment information.

3.2.6 AUSTRAC Registration

Our remittance network provider is also required to register us an affiliate. Where there is a material change to the enrolment information held by AUSTRAC, we will notify our remittance network providers within five business days.

Material changes include, but are not limited to the following:

Changes to the registration details include:

- A change in business address;
- A change in ownership; and
- Closure, suspension or termination of any agreement of by another remittance network provider.

We will notify the remittance network provider where there are changes in key personnel and a declaration that a national police certificate or national police history check has been obtained, or an application has been made for a national police certificate or national police history check for the new key personnel.

We will also notify the remittance network provider if we or our key personnel have been charged, convicted, or plead guilty/no contest to a serious criminal act such as bribery, graft, political corruption, counterfeiting, forgery, drug trafficking or distribution, fraud, money laundering, organized crime, human or organ trafficking, terrorist related crimes, or other financial crimes or crimes of dishonesty

Furthermore, we will notify our remittance network providers if we have been the subject of a civil penalty order issued under the AML/CTF Act, or is the subject of civil or criminal proceedings or enforcement action, in relation to the management of an entity, or commercial or professional activities, which were determined adversely to the person or any of its key personnel.

3.3 Risk-based systems and controls

3.3.1 Design of risk-based systems and controls

Part 8.1 of the AML/CTF Rules requires that when implementing a risk-based approach and designing risk-based systems and controls for managing and mitigating ML/TF risk, we consider:

- The types of ML/TF risk faced;
- The level of risk faced – determined by referring to risk ratings from the enterprise ML/TF risk assessment;
- The necessary mitigating controls, which should be commensurate with the level of ML/TF risk; and
- The nature, size and complexity of our business, which determines the specific controls we will utilise and whether these should be applied to customers, products or services, distribution channels and/or countries.

The ML/TF risk-based approach means that we apply AML/CTF controls on a risk-sensitive basis. The level and extent of controls applied is determined with reference to the specific ML/TF risks of our:

- Business environment
- Customer base
- Business operations
- Distribution channels
- Products and services

Our level of ML/TF risk for each of the above ML/TF risk categories is set out in our ML/TF risk assessment, which forms part of our AML Manual.

Our risk-based systems and controls are contained within this AML/CTF program and the CDD standard, which form part of our AML Manual.

3.4 Roles and responsibilities

3.4.1 Roles and responsibilities objectives

Parts 8.4 and 8.5 of the AML/CTF Rules require that our people fulfil particular roles and discharge particular responsibilities regarding AML/CTF compliance activity.

Roles and responsibilities regarding AML/CTF compliance are based on the seniority and status of the relevant employee within the organisation and are aligned to the other duties they perform.

3.4.2 Responsibilities of senior management officials

Part 8.4 of the AML/CTF Rules places responsibilities on the board and senior management.

The owner / director is responsible for ensuring that sufficient policies, procedures and resources are in place to manage the legal, regulatory and social responsibility to prevent us from being used to facilitate financial crime, including ML/TF.

The owner / director is responsible for approving the ML/TF risk assessment.

The owner / director is responsible for approving the AML/CTF program as being:

- compliant with our AML/CTF obligations; and
- appropriate to manage and mitigate the ML/TF risks we reasonably face.

The owner / director further acknowledges responsibility for maintaining and conducting ongoing oversight of the AML/CTF program to ensure that it remains compliant and effective in managing and mitigating our ML/TF risks.

The owner / director acknowledges responsibility for overseeing compliance by employees and board members with the AML/CTF program.

The owner / director also acknowledges responsibility for supporting the AML Compliance Officer in discharging his/her responsibilities, which are set out in this AML/CTF program.

The AML/CTF Compliance Officer will update the owner / director on at least an annual basis on material developments relating to the AML/CTF program or other relevant material developments in relation to ML/TF that may impact the business and its ability to comply with its AML/CTF obligations.

3.4.3 Responsibilities of the AML Compliance Officer

Part 8.5 of the AML/CTF Rules requires us to designate an employee to be the AML Compliance Officer. The AML Compliance Officer is appointed by the Director and that person must be of appropriate seniority to discharge the role and responsibilities of the AML Compliance Officer.

The AML Compliance Officer has the following responsibilities under the AML/CTF program:

- Registering with AUSTRAC and ensuring that information held by the regulator remains current;
- Ensuring that appropriate policies, procedures and controls are in place for the organisation to be compliant with AML/CTF law and regulation, and be effective in identifying, managing and mitigating ML/TF risks;
- Ensuring that knowledge on the ML/TF risks reasonably faced is appropriately maintained, including remaining abreast of changes in law, regulation, and internal practices;
- Providing leadership and contributing to a culture of AML/CTF compliance within the organisation;
- Ensuring that compliance with AML/CTF obligations is measured;
- Maintaining procedures that allow employees to report violations of the AML/CTF program to the AML Compliance Officer confidentially;
- Supporting the ongoing oversight of the Director;
- Determining if there is any matter or activity that is suspicious within the meaning of the AML/CTF Act and AML/CTF Rules, and reporting such matters to the CEO of AUSTRAC;
- Considering any AUSTRAC or other competent authority feedback regarding our ML/TF risk management performance; and
- Acting as the key contact and relationship manager for AUSTRAC and other competent authorities.

If the AML Compliance Officer is unavailable to perform his or her duties, then a nominated delegate must fulfil the role.

In addition, the AML Compliance Officer will also support the AML/CTF compliance activity undertaken by our remittance network provider(s):

- Ensuring accuracy and consistency of customer and transaction data;
- Ensuring the accuracy and completeness of SMR reports;
- Supporting completion of AML/CTF compliance reports;
- Participating and supporting compliance reviews;
- Ensuring front line staff do not process their own transactions; and

- Ensuring staff undertake relevant training modules.

3.4.4 Responsibilities of employees

All our people are also responsible for implementing aspects of the AML/CTF program. While roles and responsibilities will vary according to position, everyone is responsible for:

- Conducting our business in accordance with the AML/CTF program, and in compliance with the AML/CTF Act and AML/CTF Rules;
- Maintaining an appropriate working knowledge of the AML/CTF program;
- Following all policies and procedures associated with the AML/CTF program;
- Completing initial, and where required ongoing, AML/CTF training;
- Where relevant to their role, carrying out customer identification in line with the requirements set out in our CDD standards; and
- Reporting suspicious matters or activity to the AML Compliance Officer.

3.5 ML/TF enterprise risk assessment

3.5.1 ML/TF enterprise risk objectives

We acknowledge that our business, and our products and services, can be used for placement, layering and integration by money launderers and by people who wish to assist terrorists, both locally and overseas.

Part 8.1 of the AML/CTF Rules requires that we identify and assess the ML/TF risk that we may reasonably face as an organisation, and once we understand our ML/TF risks, ensure that our AML/CTF controls are appropriate to manage and mitigate those risks.

3.5.2 Responsibility for the enterprise ML/TF risk assessment

The AML Compliance Officer is responsible for the preparation of the enterprise-wide ML/TF risk assessment.

The owner / director is responsible for reviewing and approving the ML/TF risk assessment.

The AML Compliance Officer is responsible for regular review of the ML/TF risk assessment and making any necessary changes.

The owner / director is responsible for approving any changes to the ML/TF risk assessment.

3.5.3 Enterprise ML/TF risk assessment

The enterprise ML/TF risk assessment is completed by:

- Understanding how the nature, size and complexity of our business operations make us susceptible to ML/TF risk;
- Considering the external and internal ML/TF environment, including types of predicate crimes that might involve our customers; the internal risk relating to facilitating ML/TF and targeted financial sanctions; and the risk of non-compliance with the AML/CTF Act and the AML/CTF Rules; and
- Assessing the ML/TF risk posed by our customers; the products and services we offer; the channels we use to deliver our products and services; and the countries related to our business.

More detail about the enterprise ML/TF risk assessment methodology can be found in the appendices, which form part of our AML Manual.

We record our enterprise ML/TF risk assessment in a separate document.

3.5.4 Environmental ML/TF risk

As part of our ML/TF enterprise risk assessment, we have undertaken a risk assessment of the following categories of risks that relate to the environment in which we operate our business:

- Predicate offence risk – our vulnerability to the crimes that generate the proceeds of crime;
- Money laundering risk– our vulnerability to being involved in transactions that support money laundering;
- Terrorist financing risk – our vulnerability to being involved in transactions that support terrorist financing;
- Targeted financial sanction risk – our vulnerability to being involved in transactions that support breaching targeted financial sanctions; and

- Compliance with regulations risk – our vulnerability to not meeting legal and regulatory requirements and expectations.

We take into consideration the ML/TF risk of our business environment when designing appropriate controls to manage and/or mitigate our ML/TF risks. The AML/CTF program sets out the procedures and controls that support the management and mitigation of the ML/TF risks present in the environment in which we operate our business.

More detail about the environmental ML/TF risk assessment process can be found in the enterprise ML/TF risk assessment methodology, which together with this AML/CTF program forms part of our AML Manual.

3.5.5 Customer ML/TF risk

As part of our ML/TF enterprise risk assessment, we have undertaken a risk assessment of our customer risks at an enterprise level. This risk assessment is based upon the individual customer risk assessments undertaken as part of our CDD procedures.

Our customer enterprise ML/TF risk assessment takes into consideration the location of customers; the nature of a customer's business or occupation; whether the customer is a PEP; and whether the customer is an individual or legal entity.

We take into consideration the ML/TF risk within our customer base when designing appropriate controls to manage and/or mitigate our ML/TF risks. The AML/CTF program sets out the policies, procedures and controls that support the management and mitigation of the ML/TF risks, including the extent of customer identification required.

The ML/TF risk assessment methodology sets out how we assess the ML/TF risk of a customer.

3.5.6 Business operations ML/TF risk

Our business operations ML/TF risk assessment takes into consideration where the business operations are located, the use of third parties, and the ML/TF risks resulting from our employees.

Although AML/CTF law and regulation do not expressly require us to consider the ML/TF risks posed by our employees, we have done so to develop appropriate risk-based systems and controls for employees, as required by chapter 8.3 of the AML/CTF Rules.

We will take into consideration the ML/TF risk of our business operations when designing appropriate controls to manage and/or mitigate our ML/TF risks.

The ML/TF risk assessment methodology sets out how we assess the ML/TF risk of our business operations, any third parties we use to operate our AML/CTF controls, and our employees.

More detail about the business operations ML/TF risk assessment process can be found in the enterprise ML/TF risk assessment methodology, which forms part of our AML Manual.

3.5.7 Channel ML/TF risk

Our channel ML/TF risk assessment takes into consideration the ML/TF risk of our distribution channels, and any third parties we use to engage customers or distribute our products and services, and the circumstances under which a channel or third party represents a higher ML/TF risk.

We will take into consideration the ML/TF channel risk when designing appropriate controls to manage and/or mitigate our ML/TF risks.

The ML/TF risk assessment methodology sets out how we assess the ML/TF risk of our distribution channels, and any third parties we use to engage customers or distribute our products and services, and the circumstances under which a channel, or third party represents a higher ML/TF risk.

More detail about the channel ML/TF risk assessment process can be found in the enterprise ML/TF risk assessment methodology, which forms part of our AML Manual.

3.5.8 Product ML/TF risk

We assess product ML/TF risk using a model that assesses the flexibility of our products and services. The more flexible the product, the higher the ML/TF risk.

Flexibility is assessed by rating the product against a set of criteria. The ML/TF risk assessment methodology sets out how we assess the ML/TF risk of our products and services, and the circumstances under which a product or service represents a higher ML/TF risk.

We will take into consideration the ML/TF product risks when designing appropriate controls to manage and/or mitigate our ML/TF risks.

More detail about the product ML/TF risk assessment process can be found in the enterprise ML/TF risk assessment methodology, which forms part of our AML Manual.

3.5.9 Country ML/TF risk

Country ML/TF risk is identified by assessing countries against a set of criteria that is indicative of their vulnerability to ML/TF, and their compliance with international AML/CTF standards.

We will take into consideration the ML/TF risk of countries where our customers are located, where we have business operations, and where we use third parties when designing appropriate controls to manage and/or mitigate our ML/TF risks.

The ML/TF risk assessment methodology sets out how we assess the ML/TF risk of countries and the circumstances under which a channel or third party represents a higher ML/TF risk.

More detail about the country ML/TF risk assessment process can be found in the enterprise ML/TF risk assessment methodology, which forms part of our AML Manual.

3.5.10 ML/TF risk ratings

The results of our ML/TF risk identification and assessment, together with the ratings, are contained in our ML/TF risk assessment, which forms part of our AML Manual.

The ML/TF risk assessment rates each ML/TF risk category as presenting either significant, high, medium or low inherent ML/TF risk.

The ML/TF risk assessment also assesses the effectiveness of controls put in place to mitigate the initial ML/TF risk rating and rates each risk category as presenting either significant, high, medium or low residual ML/TF risk.

3.5.11 Ongoing enterprise ML/TF risk assessment

We are required by section 165 of the AML/CTF Act to review the enterprise ML/TF risk assessment periodically to ensure that it continues to accurately reflect the ML/TF risks posed by our business, as well as changes in business activity relevant to the ML/TF risks.

We also ensure that the risk methodology applied, and the risk attributes set out in the enterprise ML/TF risk assessment remain appropriate. This includes considering:

- An analysis of alerts from the ongoing monitoring of customer transactions;
- Industry guidance and typologies and emerging trends; and
- AUSTRAC guidance and feedback (if any).

The frequency of review is determined by the requirements of the AML/CTF Act and AML/CTF Rules.

Our enterprise ML/TF risk assessment is reviewed every 12 months, or in the event that a significant change to our ML/TF risks has been detected.

When the AML Compliance Officer undertakes a review of the ML/TF risks, they will review the enterprise ML/TF risk assessment against changes to the risk categories.

3.5.12 New designated services, channels and technologies

Part 8.1 of the AML/CTF Rules requires that the enterprise ML/TF risk assessments be varied where significant changes to the business occur (e.g. where the business wishes to introduce new products and services, distribution channels or technologies).

We will assess the inherent ML/TF risk posed by each new:

- Product and service, prior to introducing it into the business;
- Method of delivery, prior to adopting it; and
- Technology used, prior to adopting it.

If there is a material change in the enterprise ML/TF risk assessment that results in changes to the AML/CTF program, then our change

management governance process will be followed.

3.6 Governance of the AML/CTF program

3.6.1 Governance objectives

Part 8.1 of the AML/CTF Rules require that we put in place appropriate policies, procedures and controls to ensure that we are complying with our AML/CTF obligations, and that our AML/CTF compliance arrangements are, and remain, effective in identifying, managing and mitigating our ML/TF risks.

Part 8.4 of the AML/CTF Rules require that we put in place governance and oversight of the AML/CTF program.

3.6.2 Governance by senior management

The owner / director plays a significant role regarding the governance of the AML/CTF program.

The owner / director role is to oversee the AML/CTF program and ensure that it is, and remains, effective in mitigating the ML/TF risk faced and that it is compliant with the AML/CTF Act and AML/CTF Rules.

The owner / director oversight is discharged through regular and exception reporting by the AML Compliance Officer.

3.6.3 Governance by the AML Compliance Officer

The AML Compliance Officer also plays a significant role regarding the governance of the AML/CTF program and our compliance with the AML/CTF Act and AML/CTF Rules.

The AML Compliance Officer is responsible for our registration with AUSTRAC, and for keeping that information current.

The AML Compliance Officer is responsible for overseeing any action that needs to be performed as part of the AML/CTF program, and for reviewing compliance with the program periodically.

The AML Compliance Officer is responsible for ensuring that any matters of concern relating to the AML/CTF Act and AML/CTF Rules; the AML/CTF program; the ML/TF risk assessment; or compliance with AML/CTF requirements are considered and that, where necessary, a course of action is implemented.

The AML Compliance Officer is expected to escalate any material matters concerning ML/TF risk or AML/CTF compliance to the owner/ directors immediately.

The AML Compliance Officer is also responsible for determining if there are any matters or activity that are suspicious within the meaning of the AML/CTF Act and AML/CTF Rules, and for reporting such matters or activity to AUSTRAC.

3.6.4 Change management governance

The AML/CTF Rules require that we put in place appropriate change management governance to ensure that we continue to comply with our AML/CTF obligations, and that our AML/CTF compliance arrangements are, and remain, effective in identifying, managing and mitigating our ML/TF risks. We will undertake an assessment of the ML/TF risk posed if we:

- Change our business and provide other or new products or services;
- Expand our current products and services to new countries;
- Use new methods of product or service delivery;
- Introduce new or developing technologies to provide our products and services; or
- Identify new or emerging ML/TF methods relevant to our business.

Should the change be considered viable given the inherent ML/TF risk, then the AML/CTF program may be modified, including adjusting or introducing controls to manage or mitigate any additional ML/TF risk the change may pose.

The change to our business cannot be adopted until the AML/CTF program has been approved by the owner/director and any changes to any AML/CTF controls have been implemented.

3.7 CDD program

3.7.1 CDD objectives

We have designed our CDD standard in accordance with requirements set out in chapter 4 of the AML/CTF Rules. This includes:

- Collecting and verifying customer identification information;
- Undertaking simplified due diligence where the customer represents a lower ML/TF risk;
- Undertaking enhanced due diligence where the customer represents a higher ML/TF risk;
- Conducting ongoing CDD and account monitoring; and
- Managing our reliance on third parties.

Our CDD policies, procedures and controls are commensurate with the ML/TF risks we have identified as part of our individual customer ML/TF risk assessment.

We apply standard, simplified and enhanced due diligence based on the ML/TF risk of a customer.

Our customer acceptance procedures are set out in our CDD standard, which forms part of our AML Manual.

New customers must provide the identity information required by our CDD standard, and the customer's identity information must be verified to the level stipulated in the CDD standard.

Any discrepancies in information identified during customer acceptance will require a satisfactory explanation from the customer. We record how discrepancies are resolved as part of the completion of the customer acceptance procedure.

If we are not reasonably satisfied that the customer is who they claim to be, the matter must be referred immediately to the AML Compliance Officer.

We will not provide a product or service to a customer where we are not reasonably satisfied that the customer is who they claim to be.

If we are unable to collect, or a customer objects to providing, the information required as part of our CDD, the AML compliance officer will consider whether a suspicious matter report is required.

Where we refuse to accept a customer because of concerns about the identity of the customer, we do not provide reasons to the customer for the refusal. This reduces the risk of tipping off.

3.7.2 CDD Procedure

We have single CDD procedure that is aligned to the requirements placed upon us by our network providers, as well as adopting those for our independent remittance activity.

We have established transaction value thresholds that dictate what type of CDD we undertake, which range from:

- Collecting identity information, and
- Sighting official documents as verification evidence and recording the unique reference number; or
- Sighting official verification and taking copies of verification evidence; and
- asking additional questions about the transaction and the customer.

3.7.3 Remittance network provider requirements

Some of our remittance network providers specify certain restrictions on the types of customers that can use their services and also specify particular customer identity documents be provided by the customer.

These include only dealing with individuals or non-business customers in a face to face, branch office environment and only collecting identification details from original documentation and not accepting certified copies.

Where a remittance network provider places restrictions or requirements on us, we will comply with those requirements for the business we conduct through that remittance network provider.

3.8 Ongoing CDD

3.8.1 Ongoing CDD objectives

As part of the ongoing due diligence requirements set out in chapter 15 of the AML/CTF Rules, we are required to undertake:

- Beneficial owner due diligence;
- Enhanced CDD;

- CDD refresh; and
- Transaction monitoring.

Our approach to each of these activities is set out in the relevant sections of this AML/CTF program.

3.9 Enhanced CDD

3.9.1 Enhanced CDD objectives

As part of the ongoing due diligence requirements set out in chapter 15 of the AML/CTF Rules, we are required to undertake enhanced due diligence on higher ML/TF risk customers.

The objectives of enhanced CDD are to:

- Source further information in order to establish a complete understanding of the level of ML/TF risk presented by a customer;
- Understand more about the expected patterns of transactions and behaviours associated with a customer; and
- Determine whether to continue to provide products or services to a customer given the ML/TF risk posed.

Part 15.9 of the AML/CTF Rules require we undertake enhanced CDD when:

- The overall AML/CTF risk of a customer is high;
- The customer or any of its ultimate beneficial owners are foreign PEPs;
- A suspicion has arisen within the meaning of chapter 41 of the AML/CTF Act; and
- A party to a transaction is physically present in, or is a corporation incorporated in, a proscribed foreign country.

3.9.2 Enhanced CDD triggers

We will apply enhanced CDD where:

- The overall ML/TF risk of a customer has been assessed a high;
- The customer or any of its ultimate beneficial owners are foreign PEPs or high risk domestic/other PEPs;
- A suspicion has arisen within the meaning of chapter 41 of the AML/CTF Act and we have reported a suspicious matter to AUSTRAC; and
- We are entering into or proposing to enter into a transaction and a party to the transaction is physically present in, or is a corporation incorporated in, a proscribed foreign country.

3.9.3 Enhanced CDD

The enhanced CDD processes we apply involve seeking additional information about the customer and are set out in our CDD standards, which form part of our AML Manual.

Where the customer is subject to enhanced due diligence:

- We require additional approval and ML/TF risk acceptance from the senior persons responsible for the management of the business;
- We establish the source of wealth and source of funds of the customer and ultimate beneficial owners; and
- We conduct enhanced monitoring.

Any enhanced due diligence undertaken also requires review and sign off by the AML Compliance Officer (or their delegate). Depending on the outcome, the AML Compliance Officer (or delegate) will:

- Approve the customer;
- Reject the customer; or
- Advise of specific requirements for taking on the customer relationship (e.g. specific ongoing monitoring steps).

The AML Compliance Officer will also decide whether additional approval and ML/TF risk acceptance are required from the senior persons responsible for the management of the business.

We will not accept or maintain a relationship with a customer unless our requests for enhanced due diligence information are satisfactorily met by the customer.

If a customer objects to providing the information required by our enhanced CDD, the AML Compliance Officer will consider whether a suspicious matter report is required under section 41 the AML/CTF Act.

3.10 Beneficial owner due diligence

3.10.1 Beneficial owner and controller information

In order to comply with the requirements set out in chapter 4 of the AML/CTF Rules, we have, as part of our Part B CDD standards, set out the risk-based circumstances under which we should collect and verify beneficial owner and controller information relating to customers.

3.11 Unacceptable customers

3.11.1 Unacceptable customer definition

We have determined that the following customer characteristics represent an unacceptable ML/TF risk:

- Customers who are either unregulated, shell companies, or shell banks;
- Customers who do not meet the identification requirements set out in our CDD standards;
- Customers who refuse to provide information requested as part of our enhanced due diligence processes; and
- Customers or customers with an owner or controller listed in relevant sanctions lists.

3.11.2 Managing unacceptable ML/TF risk customers

We will not accept a customer or conduct a transaction for a customer who is identified as representing an unacceptable ML/TF risk, unless we are reasonably satisfied that our initial assessment was wrong and that a new assessment has resulted in a lower ML/TF risk rating.

The reason for any change in the unacceptable ML/TF risk rating of a customer must be documented.

Where an unacceptable ML/TF risk customer is identified, we will ensure that we comply with our reporting obligations under section 41 of the AML/CTF Act and, where appropriate, with relevant sanctions obligations.

3.12 Refreshing CDD

3.12.1 CDD refresh objectives

As part of the ongoing due diligence requirements set out in chapter 15 of the AML/CTF Rules, under Part 15.3 we are required to ensure that the customer identity information we hold through undertaking CDD and enhanced CDD remains accurate and up to date.

The objectives of ongoing CDD are to ensure:

- The identification of changes in a customer's identity information, should they occur; and
- A continued understanding of the level of ML/TF risk presented by a customer throughout our relationship with that customer.

3.12.2 CDD refresh

We will confirm that the identity information we hold on a customer is up to date and accurate every time a customer undertakes a transaction, by sighting an official document that confirms the identity information we hold.

We will not accept a transaction or maintain a relationship with a customer unless we can confirm that the information we hold remains up to date and accurate.

Where we are unable to confirm the customer information, the AML Compliance Officer will consider whether a suspicious matter report is required under section 41 of the AML/CTF Act.

3.12.3 CDD refresh triggers

We will refresh the information we hold on a customer when:

- Our CDD requirements materially change; or
- We become aware that the information we hold is either out of date or inaccurate.

3.13 Transaction monitoring program

3.13.1 Transaction monitoring objectives

As part of the ongoing due diligence requirements set out in chapter 15 of the AML/CTF Rules, under Parts 15.4 to 15.6 we are

required to undertake a transaction monitoring program to identify customer transactions that appear to be suspicious within the meaning of section 41 of the AML/CTF Act.

Part 15.7 of the AML/CTF Rules requires we should monitor for complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

In order to comply with Part 15.7, our transaction monitoring program uses the following techniques:

- Red flags at the individual transaction or customer interaction level; and
- Trend analysis looking at the transactions by the one customer over time, or by a group of customers who appear to be associated over time, and
- Transaction pattern monitoring by our remittance network providers.

Note: Some remittance network providers require agents to do transaction monitoring for (including but not limited) data integrity check with regards to KYC information. Moreover, patterns like, one to many, many to one, structuring of transaction to avoid internal ECDD or regulatory reporting thresholds, or any other pattern that's provided to them, on a time to time basis by remittance network providers or by the regulator or based on their own experience.

3.13.2 Monitoring for red flags

A red flag is a behaviour, action or activity that should be considered unusual. Red flags are indicators that unusual behaviour may be occurring and that employees should be on heightened alert.

We have identified the following red flags relevant to our business:

- Customers who appear overly concerned about the transaction being reported to the authorities;
- Customers who want to pay an additional fee so that they do not have to provide all the information;
- Unusual or complex transactions with no apparent economic rationale;
- Transactions that appear to be made on behalf of someone else;
- Customers who frequently make changes to their address or authorised signatory;
- Customers who do not seem to understand the product or service they are requesting or who appear vague about the identity of the beneficiary and their relationship to them;
- Customers who do not seem to understand the transaction they are undertaking or who appear vague about the identity of the beneficiary and their relationship to them;
- Customers who exhibit a low level of cooperation when providing all the customer identity information required by our CDD standards;
- Customers who exhibit a low level of cooperation when providing all the information required regarding a transaction; and
- Any other unusual behaviour by a customer, based on the normal or expected behaviour of a customer using a product or service.

With reference to the red flags for our business, all employees are required to consider whether a customer interaction or transaction is unusual or possibly suspicious and, if so, to report it to the AML Compliance Officer.

Our employees are made aware of the red flags relevant to our business as part of their AML/CTF training.

The AML Compliance Officer will review the red flags every 12 months to see if new flags should be added.

Employees must report any red flags identified to the AML Compliance Officer.

3.13.3 Monitoring and trend analysis

We conduct regular queries against our business systems and databases, looking for transactions that exhibit unusual characteristics, including:. :

- Transactions that are unusual relative to normal transaction activity (size or frequency) for a customer or peer group of customers;
- Transactions structured to avoid reporting thresholds;
- Transactions to or from higher ML/TF risk countries; and
- Transactions involving higher risk parties, such as PEPs or persons subject to sanctions.

3.13.4 Managing red flags and the results of monitoring

Where a transaction is identified against a red flag or the set of defined unusual characteristics, the AML Compliance Officer may:

- Investigate all the recent transaction history of the customer to identify anything that may be suspicious; or
- Seek further information from the customer; or
- Apply enhanced CDD; and/or
- Consider lodging a suspicious matter report.

3.14 AML/CTF awareness training

3.14.1 AML/CTF training objectives

AML/CTF training is an essential requirement set out in chapter 8 of the AML/CTF Rules. All employees are provided with AML/CTF awareness training which covers:

- Our obligations under the AML/CTF Act and AML/CTF Rules;
- The consequences of non-compliance with the AML/CTF Act and AML/CTF Rules;
- The type of ML/TF risks the business faces and the potential consequences of such risks;
- The types of suspicious activity the employee must notice and report to the AML Compliance Officer; and
- The processes and procedures provided for by the AML/CTF program to the work carried out by the employee.

The AML Compliance Officer will maintain a register which records the completion of training required of all employees.

3.14.2 Induction AML/CTF training

New employees will receive the required training before commencing duties.

Induction training may be provided via face to face, online or other delivery methods appropriate for the role of the employee.

3.14.3 Ongoing AML/CTF training

Training is refreshed every 12 months for all employees.

Ongoing training may be provided via face to face, online or other delivery methods appropriate for the role of the employee.

3.14.4 Role specific AML/CTF training

Additional AML/CTF training that is specific to an employee's role, or the ML/TF risks faced by them, may be required to be undertaken at the discretion of the AML Compliance Officer.

Employees required to undertake additional role-specific AML/CTF training will be notified and required to complete this training before commencing that role.

3.15 Employee due diligence

3.15.1 Employee due diligence objectives

Our employee due diligence program provides for appropriate screening of new employees and ongoing due diligence relating to all employees, as required by Part 8.3 of the AML/CTF Rules.

Employee due diligence is undertaken to identify and mitigate the potential ML/TF resulting from employees.

3.15.2 Initial employee due diligence

We apply the following employee due diligence program and conduct the following employee probity checks:

- CV Check; and
- A Police Record Check

We will not knowingly accept as employees, people who have police records or who have negative reports from screening that indicate an unacceptable level of ML/TF risk for our business.

3.15.3 Ongoing employee due diligence

We will repeat the following checks on our employees every time our remittance network provider contract is renewed:

- A Police Record Check.

3.15.4 Employee misconduct

Where an employee fails to follow any part of the AML/CTF program, it puts our business at serious risk of non-compliance with our AML/CTF obligations.

We consider an employee's failure to follow any part of the AML/CTF program as serious misconduct.

Based on the severity of the failure, we may reprimand, suspend or dismiss the individual immediately without any obligation to provide notice, pay in lieu of notice or provide any other compensation whatsoever.

3.16 Reporting

3.16.1 Reporting objectives

Section 40 of the AML/CTF Act requires we report certain types of transactions and matters to AUSTRAC. We comply with the reporting required by section 40 of the AML/CTF Act and the AML/CTF Rules in a timely manner and will ensure that our report meets all the specifications required by the AML/CTF Act and AML/CTF Rules.

The reporting required by the AML/CTF Act and AML/CTF Rules includes:

- Threshold transactions;
- International Funds Transfer Instructions;
- Compliance with the AML/CTF Program;
- Suspicious matters.

Chapter 8 of the AML/CTF Rules requires that we set out our systems and controls to ensure compliance with our reporting obligations.

3.16.2 Threshold transactions

Section 43 of the AML/CTF Act requires that we report cash transaction over a threshold of $10,000, and Chapter 19 of the AML/CTF Rules sets out the information we must report to AUSTRAC if we undertake a threshold cash transaction.

As we accept cash as part of our business activities, we have developed a threshold reporting procedure, which requires we submit threshold transaction reports within 10 business days. We understand that a threshold transaction arises when a single transaction involves physical currency of AUD 10,000 or more (or foreign currency equivalent). We may provide a series of services to a customer which, when combined, amount to AUD 10,000 or more (or foreign currency equivalent). We must decide whether providing a series of services constitutes a single transaction or a number of separate transactions. The decision will largely depend on the circumstances in each case. In general, a series of services can be considered a single transaction where the services share the same characteristics and purpose and are continuous. For example, and if applicable, a customer makes 2 x AUD 6,000 (cash payments) via two of our remittance network providers, this would trigger a threshold transaction which we would report.

We monitor for structuring where customers are attempting to avoid what they understand to be the threshold transaction reporting rule, including customers who may do multiple cash transactions in short time periods.

Where, through monitoring, we identify that a customer may be attempting to avoid the threshold transaction reporting rule, a suspicious matter report will be made to AUSTRAC.

Where our threshold transaction reporting obligations are shared with our remittance network providers they are agreed as part of our contract with them.

3.16.3 International Funds Transfer Instructions (IFTIs)

Section 45 of the AML/CTF Act requires that we report customer transactions, either originating from or being made to an overseas jurisdiction, to AUSTRAC. Chapter 16 of the AML/CTF Rules sets out the information we must report to AUSTRAC if we undertake an international funds transfer.

We have developed an IFTI reporting procedure, which requires we submit reports within 10 business days.

Where our IFTI reporting obligations are shared with our remittance network providers they are agreed as part of our contract with them.

3.16.4 Compliance reporting

Section 47 of the AML/CTF Act requires that we lodge compliance reports with AUSTRAC. Chapter 11 of the AML/CTF Rules sets out required for lodging compliance reports with AUSTRAC.

The AML Compliance Officer is responsible for completing and submitting our annual compliance report on or before 31st March each year.

In his or her absence, this annual report is prepared and lodged by a delegate who is nominated to act in the place of the AML Compliance Officer.

3.16.5 Unusual and suspicious matters

Section 41 of AML/CTF Act requires we report suspicious matters.

The AML Compliance Officer is responsible for forming a suspicion and completing a suspicious matter report. The AML Compliance Officer will record their decision as to whether the matter is suspicious or not, and the reasons for the decision.

If the AML Compliance Officer identifies a suspicious matter or activity, then they will lodge the required suspicious matter report with AUSTRAC within the required timeframes.

The timeframes for reporting suspicious matters or activity specified by section 41(2) of the AML/CTF Act and AML/CTF Rules are three (3) business days unless the matter involves terrorist financing, in which case it is 24 hours.

Where our suspicious matter reporting obligations are shared with our remittance network providers they are agreed as part of our contract with them.

If we file a suspicious matter report on a customer, we will review our relationship with the customer to determine whether we are prepared to continue the relationship and/or process transactions for the customer. If we subsequently decide to retain the customer, we will undertake enhanced CDD on that customer.

3.17 Record keeping

3.17.1 Record keeping objectives

We are required by chapters 20 and 29 of the AML/CTF Rules to retain and manage certain records. These records must be retained for a period of seven years but may be held for longer periods for other regulatory or business purposes.

All records created as part of compliance with our AML/CTF obligations are securely stored in physical files and/or electronically in our system.

We have ensured that all the records we retain as part of our AML compliance activity are able to be retrieved within the timeframes specified by the AML/CTF Act and AML/CTF Rules.

3.18 Tipping off

3.18.1 Tipping off objectives

Section 123 of the AML/CTF Act prohibits the disclosure of information relating to suspicious matter reports or notifying a customer or any other person that a ML/TF investigation has commenced or is in progress. The notification to the customer or anyone else that there is an investigation is called tipping off.

Once we file a suspicious matter report it is deemed that an investigation has commenced. We must therefore ensure that no one is informed about the suspicious matter report unless they are appropriately authorised.

3.18.2 Tipping off

Under no circumstances must we advise a customer or any other person that a suspicious matter report has or has not been reported.

We prohibit the AML Compliance Officer and all other employees from disclosing the contents, or even existence, of an investigation undertaken by us and any suspicious matter report to any person other than to the AUSTRAC CEO.

All employees are informed of the prohibition regarding tipping off, and it is covered in their AML/CTF training.

3.19 Regulator feedback

3.19.1 Regulator feedback objectives

Part 8.7 of the AUSTRAC Rules requires that we have in place mechanisms to receive, manage and respond to feedback and notices from AUSTRAC and other competent authorities.

3.19.2 Feedback

If applicable, we will incorporate any feedback that is provided by AUSTRAC or any other competent authority into our AML/CTF program.

Feedback will be dealt with in a timely manner as outlined in correspondence received. All amendments or additional information that affects the AML/CTF program or ML/TF risk assessment, will be attended to as required by the correspondence.

3.19.3 Notices

The AML Compliance Officer will respond promptly to all notices served by AUSTRAC or other competent authorities specified under the AML/CTF Act and AML/CTF Rules.

If we are not provided with the required notices from the regulator or other competent authorities compelling us to provide information under the relevant law or regulation, then we will not provide information, to ensure that we respect the privacy of our customers.

3.20 Independent review of the AML/CTF program

3.20.1 Independent review objectives

We are required by Part 8.6 of the AML/CTF Rules to put in place a process to commission an independent review of our AML/CTF compliance arrangements.

The independent review must:

- Assess the effectiveness of the Part A AML/CTF program in relation to the identified ML/TF risk;
- Assess whether the Part A AML/CTF program complies with the AML/CTF Act and AML/CTF Rules;
- Assess whether the Part A AML/CTF program has been effectively implemented; and
- Assess whether the Part A AML/CTF program has been complied with.

3.20.2 Independent review

We will use an appropriately qualified independent expert to conduct a review of the AML/CTF program every year. The independent expert will be instructed to:

- Assess the effectiveness of the AML/CTF program in relation to the identified ML/TF risk;
- Assess whether the AML/CTF program complies with the AML/CTF Act and AML/CTF Rules;
- Assess whether the AML/CTF program has been effectively implemented; and
- Assess whether the AML/CTF program has been complied with.

The independent review report will be provided to the owner/director on receipt.

We will address all recommendations in each independent review in a timely manner, provided that they are appropriate to our business. Unworkable recommendations will be discussed with the independent reviewer to establish recommendations that are more suitable, while still ensuring that we remain compliant with our AML/CTF compliance obligations.

Where an independent review detects material issues, the next independent review will be scheduled for six months from the completion of remediation of those issues.

3.21 Targeted financial sanctions

3.21.1 Targeted financial sanctions objectives

We acknowledge that there is a risk that our customers may be on official targeted financial sanction lists issued by the Department of Foreign Affairs and Trade (DFAT) or other relevant lists, or that our customers may transact with persons who are on these lists.

We are required by relevant law and regulation to manage the risk that our organisation and the products and services it offers could be used to breach targeted financial sanctions.

3.21.2 Customer screening

Before acceptance, each customer will be subject to a search of the relevant, targeted financial sanction lists to ensure that they are not subject to any sanction measures.

3.21.3 Transaction screening

Before each transaction is completed, each customer, the beneficiary and the remitter (where different from the customer) of the transaction will be subject to a search of the relevant, targeted financial sanction lists to ensure that they are not subject to any sanctions measures.

3.21.4 Freezing assets

Where we identify a customer who is subject to targeted financial sanction, or transaction that involves funds, financial assets or economic resources owned or controlled (directly or indirectly) by a person designated under a sanction list, we must immediately freeze the funds, financial assets or economic resources in our possession, custody or control and report the matter to the DFAT.

3.22 Other compliance requirements

3.22.1 Remittance network providers requirements

Our remittance network providers have other relevant financial crime policies and procedures which we have adopted. These policy documents are included within the Appendices of this AML Program. For example, Anti-Fraud Policies and Procedures.

3.23 Program acceptance and approval

3.23.1 AML / CTF Program acceptance and approval form

AML/CTF Program Acceptance and Approval Form

4 Customer Due Diligence Standards

4.1 Part B - Customer acceptance

4.1.1 Customer acceptance process

The customer acceptance process is designed in accordance with the requirements of relevant AML/CTF law and regulation.

The customer acceptance process must be completed before opening an account for or establishing a relationship with the customer.

Customers must provide the required identity information and be subject to appropriate identify verification for their customer type.

Where the customer is an individual, they will also be screened against the following lists:

- Politically Exposed Persons (PEP) list; and
- The Australian DFAT and OFAC targeted financial sanction lists.

Where the customer is a non-individual, the owners and controllers of the customer will also be screened against the same lists.

For all customers identified as representing a higher ML/TF risk, the enhanced CDD program determines what further information is required.

If we are not reasonably satisfied that the customer is who they claim to be, customer acceptance will not progress, and the matter will be referred immediately to the AML Compliance Officer.

If the AML Compliance Officer is not reasonably satisfied that the customer is who they claim to be, the customer will be rejected, and the AML Compliance Officer will consider lodging a suspicious matter/activity report to the relevant competent authority.

4.1.2 Ultimate beneficial owners

We consider the ultimate beneficial owner to be any individual who is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or who would be entitled on dissolution to 25% or more of the property of a legal entity.

- We will collect information regarding the identity/ies of all ultimate beneficiaries of our customers; and
- We will also take steps to verify the identity/ies of the ultimate beneficial owners of our customers.

We will identify the ultimate beneficial owners in accordance with the identification and verification process for individuals.

Where 25% or more of the ultimate beneficial ownership of a legal entity cannot be established, all those who hold the position of senior management official or equivalent will also be considered ultimate beneficial owners and will be subject to the identification and verification process for individuals.

4.1.3 Politically exposed persons (PEPs)

We will determine whether the customer or the ultimate beneficial owner of a customer, is a PEP in accordance with the criteria set out below.

All customers and customers with owners or controllers who have been identified as foreign or domestic or international PEPs represent a higher ML/TF risk. They will be subject to enhanced CDD as set out in these CDD standards.

4.1.4 PEP definition

The term PEP is used to describe someone entrusted with a prominent public function, such as a senior political figure, or an individual closely related to such a person.

A senior political figure is defined as a:

- Head of state or head of a country or government;
- Government minister;
- Senior government official;
- Judge of the High Court, Federal Court or Supreme Court, or equivalent;
- Governor of a central bank;

- Senior foreign representative, ambassador, or high commissioner;
- High-ranking member of the armed forces; and/or
- The board chair, CEO or CFO of a state-owned enterprise or international business.

The definition of a PEP includes immediate family members of senior political figures, including a:

- Spouse;
- De facto partner;
- Child or child's spouse/de facto partner; and
- Parent

The definition of a PEP also includes the close associates of senior political figures who have joint beneficial ownership of a legal entity or legal arrangement between them.
PEPs are split into three types:

- Domestic PEPs – politically exposed persons of a domestic government body;
- Foreign PEPs - politically exposed persons of a foreign government body; and
- International PEPs - politically exposed persons of an international organisation established by formal political agreement by two or more countries.

4.1.5 Certified copies

Where the documentary method of identification is employed (see verification of individuals) and original identity documents have not or cannot be provided by the customer, we require certified copies of documents.
Note: When using some remittance network providers, we must sight original documents on all occasions, therefore for these, certified copies are not accepted.

4.1.6 Authorised certifiers

The list below identifies those individuals deemed to have the sufficient status and authority to be authorised certifiers.

It is important to note, however, that individuals who are employees of the customer and fall into one of the categories below may not self-certify the customer identity documents. It is not permissible, for example, for company secretaries who are legal practitioners to certify the documents submitted to satisfy their employer's customer identity requirements.

The following individuals are considered to be authorised certifiers:

- A person who is enrolled in the court as a legal practitioner;
- A judge of a court;
- A magistrate;
- A chief executive officer of a court;
- A registrar or deputy registrar of a court;
- A justice of the peace;
- A person authorised as a notary public in a foreign country;
- A police officer;
- An agent of the postal service; and
- A consular officer or diplomatic officer.

4.1.7 Graduated due diligence

We apply a graduated approach to CDD based on the level of activity of the customer:

- Where the customer undertakes transaction under $3,500 we also record the the unique reference number and type of document provided; or
- Where the customer undertakes transaction over $3,500 we will retain a copy of the identity documents used to verify the identity of the individual.

Where the transaction is a remittance transaction over $3,500 we also collect and document:

- The customers employment
- Reason for the remittance; and

- The recipient's relationship to the customer.

We also undertake enhanced due diligence on all remittance transactions over $3,500, as well as when other triggers occur.

The details of the triggers for enhanced due diligence are set out in the enhanced due diligence section of this document.

4.1.8 Wording of certification

To certify that an identification document is a true copy of the original document, the authorised certifier must print on the copy (copying front and back of the document if appropriate) of the original document that they have sighted.

The following wording or similar wording (note that some certifiers use stamps with standard wording), must be written on the document.
For identity verification documents that contain a photograph of the signatory:

- "I certify that I have seen the original documentation and that the photograph is a true likeness and this copy is a complete and accurate copy of that original."

For other identity verification documents that do not contain a photograph:

- "I certify that I have seen the original documentation and this copy is a complete and accurate copy of that original."

The authorised certifier must sign and date the photocopy.

They must also add their name in block capitals along with their position/capacity, any registration numbers, as well as their contact address and daytime contact telephone number. If possible, they should also add the official stamp of their office.

4.2 Part B - Individuals

4.2.1 Collection of identity information

We will collect the following information about individual customers.

We will also, where required for a customer who is a legal entity, collect the following information about the individuals who are the ultimate beneficial owners or controllers.

This information must be obtained for each individual
Full name (including middle names, if provided)
Date of birth
Residential address *(Note: non-physical addresses are not acceptable)*
Nationality
Country of Birth
Occupation
Contact telephone number
If the customer is a sole trader, the principal place of business
If the customer is a sole trader, any registration number issued to the customer
If the customer has appointed an agent, the full name of each individual who purports to act for or on behalf of the customer and evidence of their authorisation. **Note: Some remittance network providers do not deal with Agents or 3rd party transactions.**

4.2.2 Additional information for remittance transactions

Where the transaction is a remittance transaction over $3,500 we also collect and document:

- Reason for the remittance; and

- The recipient's relationship to the customer.

4.2.3 Verification of identity information

AML/CTF law and regulations requires an individual's identity be verified using the most appropriate method depends on the way the customer engages with us.

As we meet our customers face to face we use documentary evidence of the customers identity data points required by either of the following:

- One photographic identification document as listed below; or
- Two non-photographic verification documents.

4.2.4 Document verification process

The individual will be advised that they need to provide the original or certified copies of appropriate documents.

Using the documents we will verify:

- The full name of each individual; and
- The residential address of the individual; or
- The date of birth of the individual.

Where the customer undertakes transaction under $3,500 we also record the unique reference number and type of document provided.

Where the customer undertakes transaction over $3,500 we will retain a copy of the identity documents used to verify the identity of the individual.

The documents that are acceptable to verify the customers identity may be limited by a remittance network provider, but are draw from the following list of primary photographic and non-photographic documents:

Acceptable Primary Photographic Verification Documents			
Driver's license:	Country/State:	Number:	Expiry date:
Passport:	Country:	Number:	Expiry date:
Government issued Photo ID card/Proof of Age:	Country:	Number:	Expiry date:

Acceptable Non-Photographic Verification Documents
Financial Benefits Statement issued by the Government within the last 12 months
Income Tax Assessment Notice issued by the National Taxation Office within the last 12 months
Rates or utility notice issued by a local government body or utility provider within the last three months
Other government issued documents containing the individual's name and current address
Bank or credit card statements containing the individual's name and current address
Payslip or letter from employer containing the individual's name and current address
Other documentary evidence that is deemed to be equivalent to the above (approval required)

4.3 Part B - Private Companies

4.3.1 Collection of identity information

We will collect the following information for private companies:

Information required
Full name of the company as registered by the local regulator
Full address of the company's registered office

Full address of the company's principal place of business
Registered number issued to the company
Full names of all directors
Information set out in the individuals' section in relation to ONE director.
Full names of verifying officers and agents, title of their position or role held, their signatures and authorising document (e.g. an Authorised Signatories list)
Each ultimate beneficial owner’s full name and date of birth or full residential address

4.3.2 Verification of identity information

For verification of the company itself (i.e. verification of the name and registered number), we will conduct a company search with the local/national company regulator.

4.3.3 Verification of verifying officers and agents

For verification of verifying officers and agents, we will collect an Authorised Signatories List detailing the names, titles and, where required, specimen signatures of the verifying officers and agents.

We will also verify the identity of ONE director of the company in accordance with the process for verifying individuals.

4.3.4 Verification of ultimate beneficial owners

We consider the ultimate beneficial owner to be any individual who is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or who would be entitled on dissolution to 25% or more of the property of the company.

Where 25% or more of the ultimate beneficial ownership cannot be established, all those that hold the position of senior managing official or equivalent will also be considered ultimate beneficial owners.

We will verify the ultimate beneficial owner/s of all private companies in accordance with the process for verifying individuals.

4.3.5 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.4 Part B - Public companies

4.4.1 Collection of identity information

We collect the following information in relation to public companies:

Information required
Full name of company as registered by corporate regulator
Full address of the company's registered office
Full address of the company's principal place of business
Company Number issued to the company by the local/national regulator
Full names of verifying officers and agents, title of their position, their signatures and authorising documents

4.4.2 Verification of identity information

For a company that is:

- A listed public company; or
- A majority owned subsidiary of a listed public company.

We confirm that the company is a listed public company by obtaining one or a combination of the following:

- A search of the relevant stock exchange;

- A public document issued by the relevant company;
- A search of the relevant corporate regulators' database;
- A search of the licence, or other records of the relevant regulator.

4.4.3 Verification of verifying officers and agents

For verification of verifying officers and agents, we will collect an authorised signatories list detailing the names, titles and, where required, specimen signatures of the verifying officers and agents.

It is not necessary to collect and verify the names of directors for listed public companies, although we may choose to do so as part of enhanced CDD if the customer is assessed as representing a higher ML/TF risk.

4.4.4 Verification of ultimate beneficial owners

It is not necessary to collect and verify the names of beneficial owners for listed public companies.

4.4.5 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.5 Part B - Trusts

4.5.1 Collection of identity information

We collect the necessary information for trusts:

Information required
Full name of the trust
Full business name (if any) of the trustee in respect of the trust
Type of trust (e.g. unit, discretionary, hybrid)
Country in which the trust was established
The full name of the Settlor of the trust
If the trustee(s) are individuals, collect the information set out in the individual standard
If the trustee(s) is a company, collect information set out in the private company's section.
In respect of each entity having the power to change the trustee, collect the information set out in the private company's section
Full name of the trust. (We must collect a full copy of the executed and dated Trust Deed or a copy of an extract and provide it with the application)
Unless the trust is widely held (10 or more unit holders), the full name of each beneficiary or a description of the class of beneficiaries of the trust:
The full names of verifying officers and agents, title of their position, their signatures and authorising document

4.5.2 Verification of identity information

For verification of the trust itself (i.e. verification of the trust name and a review of the establishment of the trust), we will review a copy of an extract of the trust deed; reliable and independent documents relating to the trust; reliable and independent electronic data; or a combination of these.

4.5.3 Simplified trustee verification process

Where a trust is regulated or has a status that means it qualifies for simplified due diligence on the trustee, we verify that the trust is:

- Registered and subject to regulatory oversight by a statutory regulator in relation to its activities as a trust; or
- A government pension or superannuation fund established by legislation.

4.5.4 Verification of the trustee(s)

Unless the trust meets the requirements for the simplified trustee verification process, we will undertake the following trustee verification

steps:

- For verification of individual trustees, we will collect and verify the identity of each trustee in accordance with the process for verifying individuals; and
- For verification of corporate trustees, we will collect and verify the identity of each trustee in accordance with the process for verifying private companies.

4.5.5 Verification of verifying officers and agents

For verification of verifying officers and agents, we will collect an authorised signatories list detailing the names, titles and specimen signatures of the verifying officers and agents.

4.5.6 Verification of the ultimate beneficial owners

We consider the ultimate beneficial owner of a trust to be any individual who holds power to appoint or remove the trustees of the trust.

For verification of the ultimate beneficial owners, we will verify the individual's identity in accordance with the process for verifying individuals.

4.5.7 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.6 Part B - Partnerships

4.6.1 Collection of identity information

A partnership is a legal relationship between two or more parties that could be either individuals or businesses. We will collect the following information for partnerships:

Information required
The full name of the partnership
The full business name (if any) of the partnership.
The country in which the partnership was established
In respect of ONE of the partners, collect the information set out in the individual section. (Where the partner is a company or other legal entity, rather than an indivdual, we will collect the necessary information for their legal entity type)
The full name and residential address of each partnership except where the regulated status of the partnership is confirmed through reference to the current membership of the relevant professional association
Partnership agreement or other verification documents
The full names of verifying officers and agents, title of their position, their signatures and authorising document

4.6.2 Verification of identity information

For verification of the partnership itself, we will collect and verify information about a partnership based on:

- A copy of the partnership agreement;
- A copy or extract of the minutes of a partnership meeting;
- Reliable and independent documents relating to the partnership;
- Reliable and independent electronic data relating to the partnership; or
- A combination of the above.

4.6.3 Verification of individual partners

For verification of individuals in a partnership, we will collect and verify the individual's identity in accordance with the process for verifying individuals.

4.6.4 Verification of corporate partners

For verification of companies in a partnership (i.e. a joint venture), we will verify the identity of the corporate partners in accordance with

the process for verifying private companies.

4.6.5 Verification of the verifying officers and agents

For verification of verifying officers and agents, we will collect an authorised signatories list detailing the names, titles and specimen signatures of the verifying officers and agents.

4.6.6 Verification of ultimate beneficial owners

This is not applicable, as the partners are the ultimate beneficial owners and are subject to verification based on their status as partners.

4.6.7 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.7 Part B - Associations

4.7.1 Collection of identity information

Associations may be incorporated or unincorporated. An incorporated association is a formalised association involving an incorporated body of persons.

An unincorporated association exists when an information association or body of persons has been created to fulfil a specific goal or purpose. An example may include a local sporting club.

We collect the following information about associations:

Information required
Full name of the association.
Full address of the association's principal place of administration or registered office (if any) or the residential address of the association's public officer or the association's president, secretary or treasurer.
The unique identifying number issued to the association upon its incorporation (incorporated associations only).
Full name and address of the chairman, secretary and treasurer (or the equivalent of each position).
In respect of any member authorised to operate the account, all information required to be collected about individuals
The full names of verifying officers and agents, title of their position, their signatures and authorising document

4.7.2 Verification of identity information

For verification of the association itself, we will undertake a verification check of the association's identity using copies of the following identification documentation obtained from the customer.

4.7.3 Verification of incorporated associations

We verify the full name and unique identifying number of the association from:

- The appropriate regulator's register pertaining to the incorporation; or
- A copy of the Certificate of Incorporation; or
- A copy of the rules of the association.

4.7.4 Verification of unincorporated associations

We verify the full name of the association from a copy of the rules or constitution of the association or the minutes/extract of the minutes of an association meeting.

4.7.5 Verification of verifying officers and agents

We will verify the identity of the chairman, secretary (or equivalent, such as the president or treasurer) in accordance with the process for individuals.

We will also verify the identity of any member that is authorised to operate the account in accordance with the process for individuals.

For verification of verifying officers and agents, we collect an authorised signatories list detailing the names, titles and specimen signatures of the verifying officers and agents.

4.7.6 Verification of ultimate beneficial owners

We consider the ultimate beneficial owner to be any individual who is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or who would be entitled on dissolution to 25% or more of the property of the company.

Where 25% or more of the ultimate beneficial ownership cannot be established, all those that hold the position of senior managing official or equivalent will also be considered ultimate beneficial owners.

We will verify the ultimate beneficial owner/s of all private companies in accordance with the process for verifying individuals.

4.7.7 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.8 Part B - Registered co-operatives

4.8.1 Collection of identity information

A registered co-operative is a business registered under the applicable legislation for co-operatives. It comprises a group of people that have formed a business to conduct a mutual endeavour for their own benefit. We collect the following information about registered co-operatives:

Information required
The full name of the registered co-operative.
Any unique identifying number issued to the co-operative when they registered with the applicable registration body.
The following addresses (collect all if available):
The co-operative's registered office or principal place of business; and
The residential address of the co-operative's secretary (if there is a secretary), or the president; or the treasurer.
The full name of the chairman, secretary, and treasurer or the equivalent officer.
The full names of verifying officers and agents, title of their position, their signatures and authorising document

4.8.2 Verification of identity information

For verification of the registered co-operative itself, we will undertake a verification check of the registered co-operative's identity using at least one of the following sources of information:

- A register maintained by the co-operative or a copy or extract of a register maintained by the co-operative;
- Any minutes of a meeting of the co-operative or a copy or extract of any minutes of a meeting of the co-operative;
- Information provided by the corporate regulator or by the applicable body responsible for the administration of the co-operative's registration;
- Reliable and independent documents relating to the registered co-operative;
- Reliable and independent electronic data relating to the co-operative; or
- A combination of the above.
- For verification of verifying officers and agents, we collect an authorised signatories list detailing the names, titles and specimen signatures of the verifying officers and agents.

4.8.3 Verification of ultimate beneficial owners

We consider the ultimate beneficial owner to be any individual who is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or who would be entitled on dissolution to 25% or more of the property of the company.

Where 25% or more of the ultimate beneficial ownership cannot be established, all those that hold the position of senior managing official or equivalent will also be considered ultimate beneficial owners.

We will verify the ultimate beneficial owner/s of all private companies in accordance with the process for verifying individuals.

4.8.4 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.9 Part B - Government bodies

4.9.1 Collection of identity information

Government bodies include statutory authorities and other bodies owned by local, state, federal and overseas governments. We will collect the following information about government bodies:

Information required
Full name of the Government Body.
Full address of the principal place of operations.
Name of all signatories
Legislation, the body, was established under.
Whether the government body is an entity, commission, charity, etc. (collect and verify).
Level of government.
The full names of verifying officers and agents, title of their position, their signatures and authorising document

4.9.2 Verification of identity information

For verification of the government body, we will undertake a search of the relevant government website and available databases for confirmation of the government body's existence.

If a government body is established under legislation, a copy of the legislation or an extract of the relevant section of the legislation will be obtained from a reliable and independent website (not from the government body's own website).

4.9.3 Verification of foreign government entities

For verification of the government body, we will undertake a search of the relevant government website and available government and other authoritative databases for confirmation of the government body's existence.

If a government body is established under legislation, a copy of the legislation or an extract of the relevant section of the legislation will be obtained from a reliable and independent website (not from the government body's own website).

4.9.4 Politically exposed persons (PEPs)

If any individual is identified as a foreign or domestic or international PEP, we will take the steps in accordance with the process for verifying individuals.

4.10 Part B - Enhanced CDD

4.10.1 Enhanced CDD approach

As set out in our AML program, the enhanced CDD process will be applied where:

- The customer undertakes a transaction remittance transaction over $3,500
- It has been determined that the level of ML/TF risk associated with the provision of a product or service to the customer is 'higher';
- It has been identified that the customer is located in a country that has been identified as a higher ML/TF risk country;
- The customer is a PEP, or an ultimate beneficial owner of the customer is a [foreign] [or domestic] [or international] PEP; or
- A 'suspicious matter/activity report' has been lodged about the customer.

Enhanced due diligence is a more detailed analysis of the customer's CDD information including, where appropriate, taking reasonable measures to identify:

- The customer's source of wealth and source of funds;
- The beneficial owner's source of wealth and source of funds.

Generic source of wealth and funds	Collect	Examples of documentary evidence
Income from employment	• Occupation • Employer's name and address • Employer's nature of business • Income per annum this year and last year	• Last 3 month's pay slips; or • Confirmation from employer of income and bonus for last 2 years; or • Recent accounts if self- employed; or • Bank statements clearly showing receipt of the last 3 months' salary payments from a named employer; or • Recent Group Certificate or Tax Return
Investment savings	• Date funds received and • from which company • Amount received • How long held	• Investment/savings certificates, contract notes or statements; or • Confirmation from the relevant investment company; or • Bank statement showing receipt of funds by investment company name • Signed letter detailing funds from a regulated accountant
Property sale	• Date funds received • Address of property • Sale value • How long property held	• Signed letter from solicitor that includes the proceeds received; or • Completed sale contract
Company sale	• Date funds received • Name and address of company • Applicant's share • Nature of business • Total sale price	• Signed letter from solicitor or regulated accountant; or • Copy of contract of sale
Inheritance	• Date funds received • Total amount received • Name of benefactor • Relationship to benefactor	• Grant of probate and/or copy of will; • Bank statements; or • Solicitor's letter
Loan	• Date funds received • Amount of loan • Name and address of loan provider	• Loan agreement; or • Recent loan statements
Gift	• Date funds received • Total amount • Details of benefactor • Relationship to benefactor • Source of donated funds	• Letter from donor confirming details of gift and acknowledging the source of the donated funds; and • Evidence of the source of funds
Other	• Date funds received • Amount • Nature of income	• Appropriate documentation that details the source of the funds or where/how the funds were generated; or • Signed letter detailing funds from a regulated accountant

We may also undertake a more detailed analysis of the customer's transactions – both past and future, including the purpose, reasons for or nature of specific transactions or the expected nature and level of transaction behaviour.

Senior management approval will also be obtained as to whether we should continue to have a business relationship with the customer.

4.10.2 Additional information – individuals

We clarify or update CDD information already collected from the customer and collect the source of funds and wealth or employment details.

We verify the source of wealth and funds, using the table below as guidance for acceptable documentary evidence.

4.10.3 Additional information - private companies

We clarify or update customer and ultimate beneficial owner information already collected from the customer.

We collect identity information for all directors in accordance with the process for individuals, and the source of funds and wealth of the customer and each ultimate beneficial owner, as well as clarifying the nature of the customer's ongoing business with us.

We verify the identity of all directors in accordance with the process for individuals, and the source of funds of the customer using the table below as guidance for acceptable documentation.

Generic source of funds	Collect	Examples of documentary evidence
Company profits	• Nature of business or activities that the company engages in and generate its revenue and profits	• Copy of latest audited accounts or • A letter from a regulated accountant giving details of company profits over the last 2 years
Loan	• Date funds received • Amount of loan • Name and address of loan provider	• Loan agreement

We verify the source of wealth of the ultimate beneficial owners using the table above as guidance for acceptable documentation.

4.10.4 Additional information – public companies

We clarify or update CDD information already collected from the customer, and collect identity information for all directors in accordance with the process for individuals, as well as clarifying the nature of the customer's ongoing business with us.

We verify the identity of all directors in accordance with the process for individuals.

4.10.5 Additional information - trusts

We collect and verify additional information in relation to each trustee as per the additional collection and verification requirements for individuals and/or companies (as relevant) as set out above.

4.10.6 Additional information – partnerships

We collect and verify additional information in relation to each partner as per the additional collection and verification requirements for individuals and/or companies (as relevant) as set out above.

4.10.7 Additional information - associations

We collect and verify additional information in relation to each individual associated with the association as per the additional collection and verification requirements for individuals as set out above.

4.10.8 Additional information - registered co-operatives

We collect and verify additional information in relation to each chairman, secretary and treasurer or the equivalent officer in the co-operative as per the additional collection and verification requirements for individuals as set out above.

4.10.9 Additional information - government bodies

We consider that government bodies will not pose a ‘high’ ML/TF risk as the body is subject to substantial regulatory and reporting oversight. Therefore, no additional information is collected or verified.

4.11 Part B - Discrepancies in identity information

4.11.1 Approach to discrepancies

Discrepancies may arise in customer identity information. Any discrepancy identified must be reported to the AML Compliance Officer as soon as practicable.

The AML Compliance Officer will review the discrepancy and decide on the best course of action. The AML Compliance Officer may direct employees or agents to obtain further customer identification as a result of discrepancies.

Some discrepancies are easily explained. Other discrepancies may be indicative of suspicious activities. On occasion, the AML Compliance Officer may determine that a suspicious matter/activity report is required as a result of a discrepancy in customer identity information.

We will not commence providing or continue to provide a product or service before all discrepancies in customer identification have been resolved.