

# Anti-Money Laundering & Counter -Terrorism Financing Legislation

April 2024

## **ANTI-MONEY LAUNDERING & COUNTER-TERRORISM FINANCING LEGISLATION**

### **OVERVIEW**

This training has been designed to provide you with an understanding of the Anti-Money Laundering and Counter-Terrorism Financing Act (2006), its impact on Latitude's products and processes and consequently your responsibility as Latitude intermediaries.

**Anti-Money Laundering and Counter-Terrorism Financing is also often referred to as AML/CTF.**

This course contains the following sections and is in addition to the Latitude Merchant Operating Guide

**Part C Section 16 – Compliance with Legislation:**

- 1. WHAT IS MONEY LAUNDERING AND TERRORISM FINANCING?**
- 2. WHAT IS THE AUSTRALIAN AML/CTF FRAMEWORK?**
- 3. WHAT ARE THE RISKS?**
- 4. WHAT DO YOU NEED TO DO?**
- 5. RED FLAGS**

Upon completing this training, you will be able to:

- Describe the obligations of Latitude under the AML/CTF Act and Rules.
- Explain the consequences of non-compliance with the AML/CTF Act and Rules.
- Identify the type of risks Latitude might face and understand the potential consequences of such risks.
- Use processes and procedures, provided by Latitude, to assist with identity verification carried out by intermediaries.

Merchants processing applications through the Merchant Portal are required to acknowledge completion of this AML/CTF training by acknowledging the training initially when logging onto the Portal or as requested thereafter.

# 1. WHAT IS MONEY LAUNDERING AND TERRORISM FINANCING?

## Money Laundering

Money Laundering is the process of converting money generated by criminal activity into seemingly legitimate funds.

Any kind of criminal activity including fraud, theft, tax evasion, drug trafficking, racketeering, prostitution, smuggling, kidnapping for ransom and threats to extort money can be a source of criminal funds. Money laundering strengthens the position of criminals in our society, undermines the global financial system and destroys Australia's reputation as a clean, effective country in which to do business.

## Terrorism Financing

Terrorism Financing is the process of using funds to support terrorist groups and perpetuate terrorism.

Funds to finance terrorism don't necessarily come from criminal activities - they can come from private contributions or donations from people who may or may not be aware that they are financing terrorism. These funds often enter the financial system in relatively small amounts – so they can be difficult for financial institutions to detect.

Terrorism financing is the lifeblood of terrorist groups. By combating the financing of terrorist acts, financial services businesses play a crucial role in the worldwide fight against terrorism.

## Targeting Financial Institutions

It's important for all of us to prevent criminal funds from entering, continuing through or leaving the financial system.

The key objective for a:

- Money launderer is to place criminal money into the financial system to hide its criminal origins.
- Terrorism financier is to take money out of the financial system and use it to finance acts of terrorism.

To launder money or finance terrorist activity, funds usually need to pass through at least one financial institution.

Latitude is always a potential target, so we must constantly guard against the risks.

## 2. WHAT IS THE AUSTRALIAN AML/CTF FRAMEWORK?

### The Act and Rules

These laws:

- Meet international standards to protect Australian businesses from being used for Money Laundering and Terrorism Financing
- Make it harder for criminals to use the profits of crime and terrorists to receive money to carry out terrorist acts.

The AML/CTF Act regulates all businesses and individuals that provide Designated Services. Credit cards including GEM Visa and GO MasterCard are considered designated services under the AML/CTF Act.

As such, Latitude:

- Is a reporting entity for the purposes of the AML/CTF Act
- Required to take a risk-based approach to preventing Money Laundering and Terrorism Financing
- Must identify, mitigate and manage the money laundering and terrorism financing risks that are posed by our products, customers, delivery methods and geographical areas of operation.
- As our Intermediaries, Latitude is relying on you to help it comply with its obligations.

### Policies, Procedures, and Individual Compliance

Financial institutions all over the world have responded to the threat of money laundering and terrorism financing by devising AML/CTF policies, procedures, and controls.

Policies and procedures can only be effective if everyone is aware that they exist and is committed to following them.

As our Intermediaries, you **must** follow the Policies and Procedures in respect to the sale of our products.

### The Regulatory Environment

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering regulator.

AUSTRAC is responsible for:

- Regulating and monitoring retail banks and other regulated businesses, including Latitude
- Monitoring compliance with applicable laws
- Gathering and disseminating information and reports from regulated businesses

- Assisting in enforcement actions
- Developing the Anti-Money Laundering and Counter-Terrorism Financing Rules. These rules specify the responsibilities that apply to Latitude as a result of the implementation of the AML/CTF Act.

## **Complying with Australian Law**

To comply with Australian law:

- YOU DO NOT need to be aware of all the details of the legislation and regulations governing the prevention of Money Laundering and Terrorism Financing
- YOU DO need to be aware of the key points – and particularly, the policies and procedures that are relevant to your role as an Intermediary of Latitude.

It is important that both Latitude and its Intermediaries take these obligations seriously.

### 3. WHAT ARE THE RISKS?

The risk that money launderers and terrorism financiers may target our organisation is real. Financial organisations across the world are constantly being targeted.

Failure to implement the required controls can lead to:

- Adverse publicity
- Damage to reputation
- Substantial fines
- Criminal charges
- Regulatory enforcement action
- Restrictions on our ability to operate freely
- The loss of our licence to operate

It can take a long time to build a relationship of trust and loyalty with a customer. This trust and loyalty can be lost in an instant.

Latitude is committed to compliance with all laws and regulatory requirements.

We all have a role to play in meeting these commitments.

Latitude is relying on you to play your part as its Intermediary.

**Remember:**

- ✓ Always follow the processes and procedures relevant to your job.
- ✓ Make sure that you know what to do if you know or suspect that any illegal activity is taking place
- ✓ If you are unsure about a process or procedure, or a customer interaction, contact Latitude for assistance. See section 5. Red Flags for further information on suspicious customer interactions.

## **4. WHAT DO YOU NEED TO DO?**

### **Identifying Customers**

The principal objectives of our Know Your Customer (KYC) procedures are:

- To ensure that we accept only legitimate and bona fide customers, that is, that we are reasonably comfortable that we know who they are and that there is no suspicion surrounding the application
- To ensure that we properly identify our customers and understand the risks they may pose for us.

### **Accepting New Customers**

At a minimum, customer identification includes:

## **COLLECTING AND VERIFYING INFORMATION**

The Merchant Portal will guide you on how to collect, verify and record customer information in order to meet AML/CTF requirements.

When completing the customer identification procedure, you should also consider:

## **DOCUMENTATION**

- Does the customer possess all the required documents in the proper form?

## **AUTHENTICITY**

- Are the documents and information provided original and authentic?
- Do the signatures match?
- Do photographs appear to be of the same person?
- Are there several or unusual fonts on the document?
- Does the document appear to have been altered or forged?

## **IDENTITY**

- Is the customer actually the stated individual?

## **CONSISTENCY/ CREDIBILITY**

- Is the information provided by the customer consistent? Are the customer's explanations credible?
- If you have any concerns relating to a customer's application or identification procedure, immediately report this to Latitude. See section 5. Red Flags below for more information.

## 5. RED FLAGS

### Potentially Suspicious Matters

Potentially Suspicious Matters are events, patterns of behaviour or transactions that are unusual or that could indicate that a customer is involved in money laundering or terrorism financing.

They arise when you have reasonable grounds to suspect that a customer, or a potential customer, is involved in criminal or terrorist acts.

### Red Flags

Potentially Suspicious Matters can involve (though are not restricted to):

- A customer is unusually nervous
- A customer is unable or unwilling to provide personal background information
- A customer provides unusual, suspicious, or falsified identification or income documentation
- A customer discusses our record keeping or reporting duties with the apparent intention of avoiding them
- Cash-intensive transactions.

All of us must be alert to potentially Suspicious Matters. Latitude must report any Suspicious Matters to the Australian Transaction Reports and Analysis Centre (AUSTRAC). These reports must be made within tight deadlines and failure to meet these deadlines could result in regulatory action.

To enable Latitude to meet its obligations, it is important that you let us know immediately if you encounter or identify something that is potentially suspicious.

### Tipping Off

If you do identify a potentially suspicious matter regarding a customer or transaction, you must **never** inform an individual that they, or their activities, are the subject of a suspicion or a report to Latitude and potentially AUSTRAC, or an investigation into money laundering or terrorism financing.

“Tipping off” or informing a customer about any suspicion or report to AUSTRAC could compromise an investigation. “Tipping Off” is an offence under Australian Law, punishable by up to 2 years imprisonment and/or a fine.

For this reason, you should never inform a customer, or anyone else, that a report has been made about them or their activities and you should never discuss potentially suspicious activities with anyone other than:

- The designated contact at Latitude
- Your manager or supervisor.

If information that you provide forms part of a suspicious matter report to AUSTRAC about a customer, your identity will be protected.

Latitude has developed policies and procedures (“Extension 500”) that articulate the process



that you need to follow if you identify potentially suspicious activity. You must ensure you follow these procedures.

For more information, consult your Latitude Representative.

### **“Extension 500” – Raising Red Flags**

To assist you in meeting your Legislative requirements, Latitude has developed a process to ensure you can report any potentially suspicious activity to us safely and without risk of “Tipping Off” the customer.

First, move to a secure area where the customer and others cannot hear you. Contact Latitude on 1300 361 921 for GO MasterCard / Gem Visa / CreditLine and advise our Representative that you need to be put through to “Extension 500”.

The Latitude Representative will ask you closed-ended questions to ensure that you can provide us the necessary details without making the customer aware of your concerns.

The Latitude Representative will then advise you of the next steps to take and help you manage the situation safely.

## APPENDIX 1: LATITUDE ID REQUIREMENTS

### Identifying customers

As discussed above, Latitude must establish and verify the identity of the people who utilise our products and services. This process is called Know Your Customers or KYC.

Additionally, to be eligible to apply, customers must be:

- Over 18 years of age, and
- Australian resident – OR – The applicant must intend and have visa permission to stay in the country for at least the next 12 months.

**In all cases, you must sight, verify, and record the customer's identification to meet our obligations under AML Legislation. Staff Identification (Staff/Payroll ID and Full Name) must be completed on the application in order to confirm this requirement has been met.**

## Which documents

There are **2 options** for the customer to provide ID for you to verify:

Option 1 – only ONE ID document is required, any one of:		You must check and ensure:
<ul style="list-style-type: none"> <li>• Australian Driver’s Licence</li> <li>• Australian Digital Driver's License* (SA &amp; NSW only)</li> <li>• Australian Learner’s Permit</li> <li>• Proof Of Age card with Address**</li> <li>• NSW Photo Card showing the customers full name, address, and DOB</li> </ul> <p>* Can only be used in issuing state (i.e., SA digital driver’s license can only be used in SA)</p> <p>**Where the proof of age card does not have an address, customers must supply documentation from Option 2.</p>		<ul style="list-style-type: none"> <li>✓ ID is current and original</li> <li>✓ Name (in correct order), date of birth and address (current or previous) matches the application details</li> <li>✓ All required ID details are correctly entered in the Personal Details – Identification section of the customer’s Application within Merchant Portal.</li> </ul> <p>It is not required to keep a copy of the ID document</p>
Option 2 – TWO ID documents are required		
Any ONE of these ID documents	PLUS any ONE of these ID documents showing the customer’s current residential address:	
<ul style="list-style-type: none"> <li>• Australian Passport with photo ( that has not been expired for more than 2 years)</li> <li>• Foreign Passport with Accredited Translation (that is current and not expired)</li> <li>• Pension Card</li> <li>• A Birth Certificate or Birth Extract that has been issued by an Australian State or Territory.</li> </ul>	<ul style="list-style-type: none"> <li>• CentreLink Statement (less than 12 months old)</li> <li>• Rates notice (less than 3 months old)</li> <li>• Utility bill               <ul style="list-style-type: none"> <li>- gas / electricity / water/ home phone/ mobile phone (less than 3 months old)</li> </ul> </li> <li>• Taxation Notice of Assessment (less than 12 months old)               <ul style="list-style-type: none"> <li>- <b>If a Taxation Notice is used, you must use the Document Number, not the Tax File Number.</b></li> </ul> </li> </ul>	

## **Record keeping**

- ✓ It is your responsibility to ensure all information is recorded in the Merchant Portal as detailed on the customer's ID document/s.
- ✓ Latitude will keep and maintain customer records for the duration of the customer relationship and 7 years after the relationship has ended.