Real Estate

Continuing Professional Development

Anti-Money Laundering: Your compliance requirements

Estimated time needed: 1 hour 30 minutes

Name:

Version 2.0

04 February 2019

Contents

Real Estate Continuing Education 2019, Anti-Money Laundering: Your compliance requirements, covers the following information:

Learning objectives

- Introduction: reviewing what money laundering means (including relevant information around Financing of Terrorism)
- Understanding associated legislation and how it applies to real estate
- Understanding the role of the Department of Internal Affairs (DIA)
- Knowledge and understanding of compliance requirements as a reporting entity
- Understanding customer due diligence obligations
- Understanding reporting requirement obligations
- Reviewing relationships with other Anti-Money Laundering (AML) entities
- Recognising 'red flags'
- Understanding DIA expectations for compliance

Introduction to money laundering

Money laundering in New Zealand

The Ministry of Justice describes money laundering as:

> 'the process criminals use to 'clean' the money they make from crimes such as fraud, dealing in illegal drugs and tax evasion.
>
> By making the money look like it comes from a legitimate source, they can cover their tracks and avoid detection.'
>
> https://www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/what-is-aml-cft/

In the criminal world *cash is king* and money laundering is an essential process to change 'dirty' money into 'clean' money.

This is achieved through buying and selling assets, for example property and expensive goods such as cars, boats and jewellery. Or by channelling funds through financial structures (for example companies, trusts).

Money laundering often involves a complex series of transactions; moving money around different parts of the financial system, thereby disguising its origin. This makes it harder for authorities to find out where 'dirty' money has originated from, and from whom, and more difficult to catch and prosecute criminals and seize illegally gained money and/or assets.

Money laundering is happening every day across New Zealand. According to the New Zealand Police's Financial Intelligence Unit (FIU), there is reportedly around $1.35 billion of funds from fraud and illegal drugs laundered through legitimate businesses within New Zealand every year.

The effects of this reach far wider than just those involved directly with money laundering. There is a significant human toll on victims and their families, and serious harm to communities which are exposed to crimes that generate 'dirty' money.

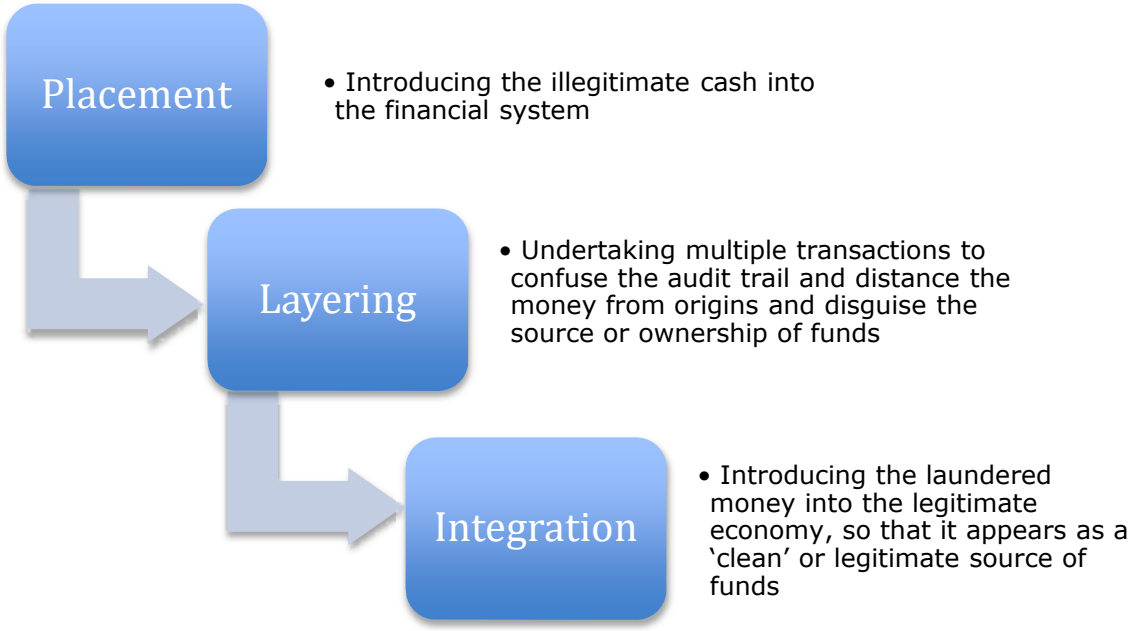
Ease of money laundering enables organised crime to flourish and causes potential economic damage and a tarnished reputation for New Zealand. Many around the world view New Zealand as a safe country. However, criminals view New Zealand as a 'soft' option to launder money and do so by:

- Exploiting weak points in the financial network
- Targeting businesses or professions that don't confirm customers' identities, or don't have the right checks and balances in place to detect suspicious transactions, activities, behaviour or financial arrangements (the financing of terrorism uses similar techniques)

How is money laundered?

Money laundering is typically actioned in a three-stage process:

1. Placement
2. Layering
3. Integration



Note:

At the time of writing there were no examples of money laundering within the real estate sector in New Zealand.

However, two examples involving financial institutions provide insight into how money laundering is actioned, utilising the three-stage process as outlined above.

Breach of AML/CFT Act: example 1

In September 2017 a remittance and money transfer company based in Auckland was ordered to pay $5.3 million in penalties for anti-money laundering breaches.

The Department of Internal Affairs took action against the company in the High Court, alleging 'the company had failed to take steps required in 1588 transactions involving more than $100 million in 2014'.

The judge found that the company failed to keep appropriate records of the transactions and failed to record the identity of 362 customers involved in the laundering activity.

https://www.stuff.co.nz/business/97408647/auckland-company-ordered-to-pay-53m-in-penalties-over-antimoney-laundering-breaches (i.stuff.co.nz; September 29, 2017)

This breach example demonstrates the three-stage process of money laundering:

- Use of a financial business – *Placement*
- Multiple transactions by multiple individuals – *Layering*
- Laundered money re-introduced into the legitimate economy, making it appear 'clean' - *Integration*

Case: [2017] NZHC2363
http://www.nzlii.org/cgi-bin/sinodisp/nz/cases/NZHC/2017/2363.html?query=Ping%20An

Case: [2018] NZHC530
http://www.nzlii.org/cgi-bin/sinodisp/nz/cases/NZHC/2018/530.html?query=Ping%20An

Notes

Breach of AML/CFT Act (Australia): example 2

In August 2017 AUSTRAC (Australia's financial intelligence and regulatory agency) initiated proceedings against the Commonwealth Bank of Australia (CBA) for 'serious and systemic non-compliance with the *Anti-Money Laundering and Countering Financing of-Terrorism Act 2006* (AML/CFT Act)'.

The action taken by AUSTRAC alleges over 53,700 contraventions of the AML/CFT Act 2006 by the CBA.

A summary of alleged breaches includes:

- CBA did not comply with its own AML/CFT program, because it did not carry out an assessment of the money laundering and terrorist financing (ML/TF) risk of IDMs (intelligent deposit machines /ATMs) before their rollout in 2012. CBA took no steps to assess the ML/TF risk until mid-2015 - three years after they were introduced.

- For a period of three years, CBA did not comply with the requirements of its AML/CFT program relating to monitoring transactions on 778,370 accounts.

- CBA failed to give 53,506 threshold transaction reports (TTRs) to AUSTRAC on time for cash transactions of $10,000 or more through IDMs [ITMs] from November 2012 to September 2015.

- These late TTRs represent approximately 95 per cent of the threshold transactions that occurred through the bank's IDMs [ITMs] from November 2012 to September 2015 and had a total value of around $624.7 million.

- AUSTRAC alleges that the bank failed to report suspicious matters either on time or at all involving transactions totalling over $77 million.

- Even after CBA became aware of suspected money laundering or structuring on CBA accounts, it did not monitor its customers to mitigate and manage ML/TF risk, including the ongoing ML/TF risks of doing business with those customers.

http://www.austrac.gov.au/media/media-releases/austrac-seeks-civil-penalty-orders-against-cba

In June 2018 it was reported (by ABC News) that an out of court settlement had been reached and that 'the CBA had agreed to pay the biggest fine in Australian corporate history'; $700 million plus legal costs.

At the time of reporting, the Federal Court (of Australia) was still required to accept the terms of the agreement.

The report further stated that:

- The bank failed to properly monitor transactions on over 770,000 accounts over a period of three years, to check for money laundering red flags
- The bank admitted to the late filing of 149 suspicious matter reports
- The bank breached its obligations to perform checks on 80 suspicious customers
- Transaction monitoring did not operate as intended on a number of accounts
- AUSTRAC also exposed 14 occasions where the CBA failed to properly assess risks related to its IDMs

The Chief Executive of AUSTRAC stated:

> 'I hope this result alerts the financial sector to the consequences of poor compliance and reinforces that businesses need to take their obligations (AML/CFT compliance) seriously'

http://www.abc.net.au/news/2018-06-04/commonwealth-bank-pay-$700-million-fine-money-laundering-breach/9831064 - June 2018

Notes

Risk of money laundering activities using real estate

According to the Department of Internal Affairs (DIA)

> 'real estate is an attractive option for money launderers because it can be used both in layering and integrating proceeds of crime by re-entering the legitimate economy.'
>
> 'And the inherent risk of money laundering and financing of terrorism within the real estate sector, according to the DIA, is *medium to high*.'

Some examples of this risk include:

- **Purchase values of real estate are significantly large**, so it provides an option to launder large amounts of money without attracting suspicion
- **Numerous bank transfers can be made from overseas accounts** for balance payments for purchasing property
- Once real estate has been bought, it can be used as **security for a loan**
- Once real estate has been bought, **it can be resold**, and the sale **proceeds integrated into the legitimate economy**
- Buy real estate and **on-sell immediately**; again, with the intention of integrating sale proceeds into the 'legitimate economy'
- Carry out a **series of transactions** with a bank or business that (individually) are **below the monetary thresholds that trigger money laundering 'red flags'** - less than $10,000 cash transaction, but cumulatively amount to large sums
- A sale of property can be **used to explain a source of funds**
- Through **beneficial ownership,** by hiding their identity using companies and/or trusts to own or buy assets

Those involved in the financing of terrorism use similar methods to money launderers by channelling funds to violent causes and disguise who is providing and receiving the money.

NZ legislation & real estate

Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (*the AML/CFT Act*)

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (*the AML/CFT Act*) was passed to tackle the increasing exposure New Zealand is facing with money laundering and terrorism financing.

It set in place obligations on New Zealand financial institutions and casinos to detect and deter money laundering and terrorism financing through establishing monitoring and reporting compliance requirements (refer to Appendix 1 – AML/CFT Act, Section 3 Purpose).

The AML/CFT Act included an initial 'Phase 1' which encapsulated certain businesses within New Zealand. Businesses subject to the Act are referred to as a 'reporting entity'.

Important note:

All reporting entities are required to comply with strict monitoring and reporting requirements as set out in the AML/CFT Act.

The initial focus (Phase 1) was on casinos, and other financial institutions such as banks, fund managers and debt collectors.

However, in Phase 2 the AML/CFT Act broadened its scope of reporting entities and included *designated non-financial businesses or professions,* which includes *real estate agent*.

AML/CFT Act Section 5 Interpretation (part)

designated non-financial business or profession means—

> (a) a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, **a real estate agent**, or a trust and company service provider, who, in the ordinary course of business, carries out 1 or more of the following activities: …

The 'activities' that a real estate agent carries out is further stated within this definition as:

> 5(a)(v) providing real estate agency work (within the meaning of section 4(1) of the Real Estate Agents Act 2008) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008)

According to the Real Estate Agents Act, 2008 a real estate agent is:

Real Estate Agents Act 2008 Section 4 interpretation

4(1) **real estate agency work or agency work** –

(a) means any work done or services provided, in trade, on behalf of another person for the purpose of bringing about a **transaction**; and

(b) includes any work done by a branch manager or salesperson under the direction of, or on behalf of an agent to enable the agent to do the work or provide the services described in paragraph (a)

transaction – means the sale, purchase, or other disposal or acquisition of a freehold or leasehold (other than a residential tenancy) interest in land, a registerable licence, an occupancy right, or a business

Real Estate Agents as 'Reporting Entities' and captured activities

From 1 January 2019, the AML/CFT Act applies to all real estate agents. Real estate agents are now 'reporting entities' and are required to fully comply with the AML/CFT Act.

Therefore, **ALL licensees** who work for a real estate agent and in the ordinary course of business carry out real estate agency work, and manage client funds in relation to that activity, are required to fully comply with the AML/CFT Act.

For example, receiving deposit funds from a purchaser or someone on behalf of the purchaser, holding them in the agency's trust account and then releasing the funds to the person entitled to them, is *managing client funds* and an activity captured by the AML/CFT Act.

Except for some commercial property management activities[1], **property management activities** and managing client funds for that purpose are **not** captured by the AML/CFT Act. For example, receiving rental or lease payments on behalf of a client is *managing client funds for the purpose of property management activity* as defined in regulation 21B of the AML/CFT (Definitions) Regulations, and therefore is an activity that is not captured by the AML/CFT Act.

Key Point

Remember, criminals use various money laundering opportunities to convert 'dirty' money, made through criminal activities, into 'clean' money, exploiting weaknesses within the financial network, including the purchase of assets such as property.

To successfully tackle the increasing exposure New Zealand faces with money laundering and terrorism financing, it is essential that all reporting entities that could be exploited by the criminal world are included in the AML reporting compliance requirements.

[1]The exclusion of property management activity does not cover 'acting, or offering to act, for reward in respect of the negotiation, grant approval, or assignment of a tenancy agreement for commercial premises (whether described as a lease, tenancy agreement, right to occupy, or otherwise)'. Anyone engaging in these activities has full obligations under the AML/CFT Act in relation to these activities.

The Act also applies to other Phase 2 reporting entities who are in a non-financial designated business or profession as follows:

- Lawyers and Conveyancers (from 1 July 2018)
- Businesses that provide trust and company services (from 1 July 2018)
- Accountants (from 1 October 2018)
- **Real Estate Agents (from 1 January 2019)**
- Businesses trading in high-value goods (from 1 August 2019)
- Sports and racing betting (from 1 August 2019)

The staggered approach for Phase 2 reporting entities was to ensure that they had time to understand their obligations under the Act including:

- Appointing a compliance officer, and
- Developing, maintaining and auditing their risk assessment and compliance programme, and
- Knowing who their customers are, and on whose behalf they act, and completing the required level of identity verification i.e. customer due diligence, and
- Reporting large cash transactions, and
- Reporting suspicious activity, and
- Submitting an annual report to the Department of Internal Affairs.

Money laundering offence

Before we look in detail at the compliance requirements of a reporting entity, it is important to clarify what constitutes a *money laundering offence*.

The AML/CFT Act states:

> **5 Interpretation**
>
> **'money laundering offence** means an offence against section 243 of the Crimes Act 1961 or section 12B of the Misuse of Drugs Act 1975 or any act committed overseas that, if committed in New Zealand, would be an offence under those sections of those Acts'

Section 243 of the Crimes Act 1961 refers to the crime of **Money laundering** and provides a lengthy analysis of money laundering activities, which include:

- **Act** – includes an omission
- **Conceal** – in relation to property (real or personal)
    - to conceal or disguise the nature, source, location, disposition, or ownership of the property or of any interest in the property
- **Deal with** – in relation to property (real or personal)
    - to dispose of the property, whether by way of sale, purchase, gift or otherwise
    - to transfer possession of the property
- **Interest** – in relation to property (real or personal)
    - a legal or equitable estate or interest in the property; or
    - a right, power, or privilege in connection with the property
- **Offence** – means an offence that is punishable under New Zealand law whether committed in New Zealand or overseas
- **Proceeds** – in relation to an offence, means any property that is derived or realised, directly or indirectly, by any person from the commission of the offence
- **Property** – means real or personal property of any description, whether situated in New Zealand or elsewhere and whether tangible or intangible; and includes an interest in any such real or personal property

Section 243A provides that even if an offence was committed by someone else, a person may be charged if they have in their possession property that is the proceeds of an offence, and they intend to engage in money-laundering knowingly or being reckless as to whether that property is proceeds of an offence.

All licensees should be fully aware of these areas of money laundering within the real estate industry.

The role of the Department of Internal Affairs (DIA)

A key aspect of the AML/CFT Act is the establishment, and associated role of **supervisors** for the purposes of monitoring and enforcing compliance requirements of reporting entities.

An **AML/CFT supervisor** in relation to a reporting entity, means the person referred to in section 130(1) of the AML/CFT Act (refer to Appendix 1 – Section 130 AML/CFT supervisors) that is responsible for supervising the reporting entity.

Section 130 of the AML/CFT Act stipulates a three-fold allocation of supervisory responsibility to existing public entities and government departments.

The areas of supervisory responsibility are allocated as follows:

- **Reserve Bank of New Zealand** – supervises banks, life insurers, and non-bank deposit takers. Manages monetary policies
- **Financial Markets Authority** – supervises issuers of securities, fund managers, brokers and custodians, financial advisers. Regulates capital markets and financial services
- **Department of Internal Affairs** – supervises the New Zealand Racing Board, casinos, non-deposit taking lenders, money changers, high-value dealers, and any other reporting entities not supervised by the Reserve Bank or the Financial Markets Authority

Note: Each reporting entity may only have one (1) AML/CFT supervisor (refer Section 130(5)).

Note

The Department of Internal Affairs (DIA) is a public service department charged with a number of functions including administering passports, citizenship, lottery grants; registering births, deaths, marriages and civil unions; providing support services to ministers of the Crown; and advising the government on various policies and issues.

The supervisor for real estate agents

AML/CFT Act, Section 130(1)(c) states that the Department of Internal Affairs (DIA) is tasked with supervising *designated non-financial business or professions,* and is therefore, the **supervisor of real estate agents.**

Under the AML/CFT Act, real estate agents are a *designated non-financial business or profession*.

Functions of supervisors

The functions of a supervisor are set out in **AML/CFT Act - section 131** (refer to Appendix 1) and include:

- Monitor and assess the level of risk of money laundering across the reporting entities it supervises
- Monitor the reporting entities for compliance with the AML/CFT Act and regulations
- Ensure a supervisory programme is developed and implemented
- Provide guidance to help reporting entities to comply with the AML/CFT Act
- Investigate reporting entities and enforce compliance
- Co-operate on a domestic and international level to ensure consistent, effective, and efficient implementation of the Act

Codes of practice

The DIA is required 'to prepare codes of practice for relevant sectors if directed to do so by the Minister responsible for the AML/CFT supervisor' (section 63(1) – Appendix 1).

The purpose of a code of practice is to provide a statement of practice that assists reporting entities to comply with their obligations under the AML/CFT Act and regulations (section 63(2) – Appendix 1).

DIA Guidelines

The DIA also provides guidelines for reporting entities in sectors it supervises.

In August 2018 the DIA released the first guideline for real estate. It was updated in December 2018 and will be regularly updated as new information becomes available or new legislation or case law changes any AML/CFT obligations. This guideline provides essential information for ALL LICENSEES and is located on the DIA website.

https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines#Real-Estate

It is important that all licensees bookmark this web page and refer to the online content regularly to ensure the most up-to-date information is accessed.

Powers of supervisors

The AML/CFT Act provides supervisors with extensive powers to fulfil their role.

Section 132 (refer to Appendix 1 – Section 132 - Powers) sets out in detail the parameters of powers. Note should be taken of section 132 subsection (1) which states:

> 132 (1) An AML/CFT supervisor has **all the powers necessary** to carry out its functions under this Act or regulations

It is important to remember that the powers necessary to carry out their function as supervisor include the power to:

- Have full access to all records, documents or information it deems relevant
- Conduct on-site inspections (refer to section 133)
- Provide guidance
- Produce guidelines
- Prepare codes of practice
- Provide feedback on compliance
- Undertake any other activities necessary

Section 133 outlines additional details around supervisors' powers to conduct on-site inspections; particularly subsection (1):

> 133 (1) An AML/CFT supervisor may, at any reasonable time, enter and remain at any place (other than a dwelling-house or a marae) for the purpose of conducting an on-site inspection of a reporting entity.

Questions:

Read the following statements and decide whether they are true or false.

1. The Department of Internal Affairs (DIA) is responsible for supervising real estate agents as 'reporting entities', to ensure their compliance with statutory obligations under the AML/CFT Act.

   True / False

2. The DIA is the only supervisory body designated under the AML/CFT Act.

   True / False

3. The functions of a supervisor are **solely** to monitor the reporting entities for compliance with the AML/CFT Act and regulations.

   True / False

4. The supervisor is able to provide guidance to the reporting entities it supervises.

   True / False

5. A supervisor has the power to investigate reporting entities it supervises and enforce compliance with the AML/CFT Act and regulations.

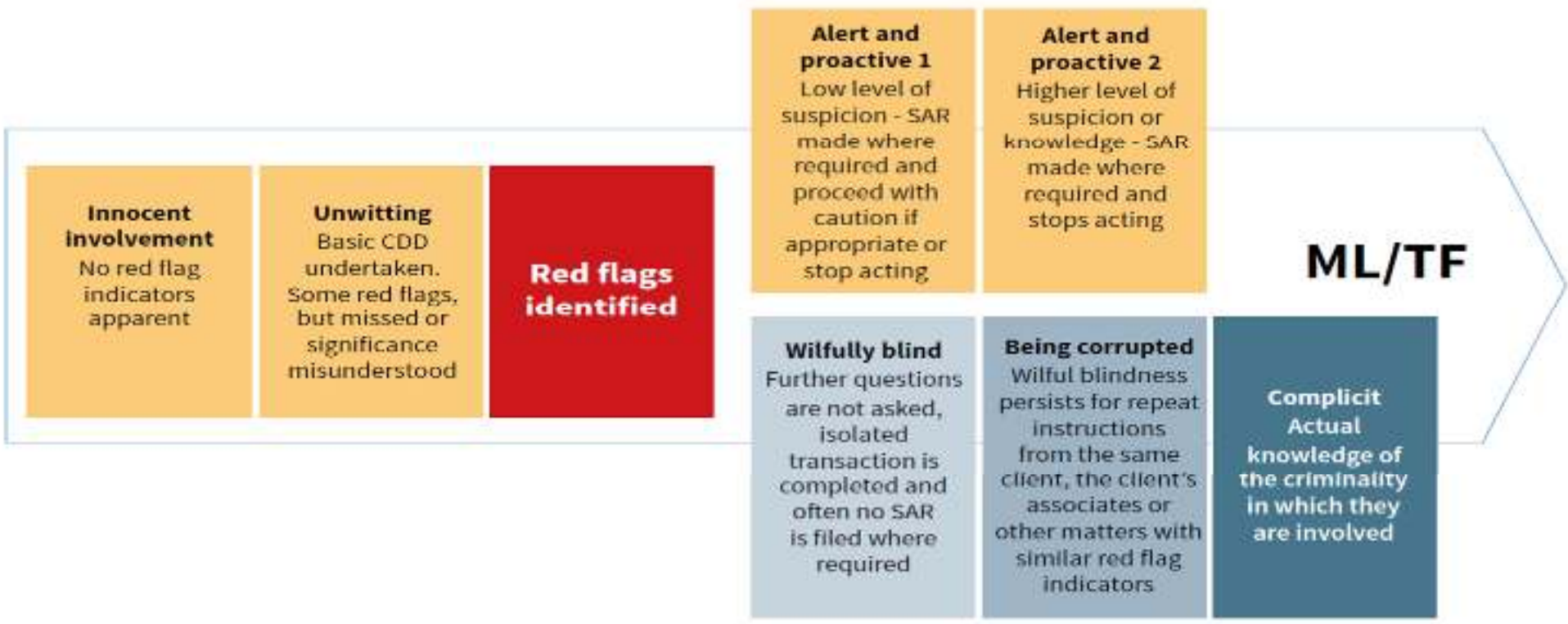
   True / False

6. The AML/CFT Act provides supervisors with all the powers necessary to carry out its function.

   True / False

7. An AML/CFT supervisor may, at any reasonable time, enter and remain at any place (other than a dwelling-house or a marae) for the purpose of conducting an on-site inspection of a reporting entity.

   True / False



Source: DIA Guidelines December 2018

Real estate agents are often referred to as *gatekeepers* of the [real estate] transaction. This is also true about AML/CFT exposure.

The diagram above is provided by the Financial Action Task Force (FATF), the inter-governmental body that sets global AML/CFT standards. It describes the two potential trajectories of real estate professionals' involvement in, and compliance with money laundering and terrorist financing (ML/TF).

SAR – Suspicious Activity Report

Reporting entity: compliance requirements

As previously mentioned, a real estate agent is deemed to be a reporting entity as defined by the AML/CFT Act.

Section 48 of the Real Estate Agents Act 2008 authorises the (agent) licensee to carry out real estate agency work on his or her own account.

Furthermore, **section 49 of the Real Estate Agents Act 2008** authorises the holder of either a salesperson's licence or a branch manager's licence to carry out real estate agency work **for or on behalf** of the agent licensee.

It should be noted that auctioneers of real estate, whether licensed or registered, are also deemed to be reporting entities and will be required to comply with the requirements of the AML/CFT Act.

When we look at the statutory requirements of reporting entities, it is important to remember that these requirements apply to all licensees.

Statutory requirements of reporting entities

The AML/CFT Act, Section 4 - Overview provides for AML/CFT requirements and compliance. Specific relevant parts (refer to Appendix 1 - section 4 Overview, Part (3) for an excerpt of the section) include:

- Provisions dealing with requirements on reporting entities to **conduct due diligence** on customers and certain other persons
- **Prohibitions** on establishing or continuing business relationships and setting up facilities in certain circumstances
- Provisions dealing with requirements on reporting entities to **report suspicious activities** and their protection
- Requirements on reporting entities to **report** certain prescribed transactions
- Requirements on reporting entities to **keep records** (including storage and destruction of records)
- Reporting entities' internal **policies and procedures**
- A requirement to carry out a **risk assessment**
- Requirements to have **AML/CFT programme** to detect and manage the risk of money laundering and financing of terrorism, to review and audit that programme; and
- The requirement to **report** on the risk assessment and programme
- The requirement to appoint a **compliance officer**.

In summary, the AML/CFT Act requires reporting entities to:

- Undertake a Risk Assessment to identify the money laundering and financing of terrorism risks that you could expect in the course of running your business
- Develop an AML/CFT Programme that includes procedures to detect, deter, manage and mitigate money laundering and the financing of terrorism
- Appoint a Compliance Officer to administer and maintain the AML/CFT programme
- Undertake Customer Due Diligence processes to verify the identity of your client and others as required
- Report Suspicious Transactions
- Report Prescribed Transactions
- Establish Auditing and Annual Reporting systems and processes

Note

A reporting entity is required to undertake a risk assessment, develop an AML/CFT programme, appoint a compliance officer (AMLCO), report annually on its risk assessment and compliance programme and audit the risk assessment and compliance programme every second year.

While some of these obligations are carried out at a management level, it is **important that all licensees are aware of, and understand, these obligations as they relate to their day-to-day real estate agency work**.

Customer due diligence and suspicious transaction reporting (Suspicious Activity Reports (SARs) and Prescribed Transaction Reports (PTRs)) will be covered separately later.

AML/CFT Requirements

Risk Assessment

The DIA refers to the AML/CFT as a regulatory system that is *risk-based*.

This means that every real estate agency must carry out an assessment of the risk it is exposed to from potential money launderers and terrorist financers.

AML/CFT Act Section 58 outlines the requirements for undertaking a risk assessment (refer to Appendix 1 – Section 58 Risk Assessment).

The key priority of the reporting entity is to:

> 58 (1) '……..undertake an assessment of the risk of money laundering and the financing of terrorism (a risk assessment) that it may **reasonably expect to face** in the course of its business.'

When undertaking a risk assessment, regard should be given to:

> 58 (2) '….(a) the nature, size, and complexity of its business; and
>
> (b) the products and services it offers; and
>
> (c) the methods by which it delivers products and services to its customers; and
>
> (d) the types of customers it deals with; and
>
> (e) the countries it deals with; and
>
> (f) the institutions it deals with; and
>
> (g) any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to risk assessments; and
>
> (h) any other factors that may be provided for in regulations.

The Risk Assessment **must** be in writing and

> 58 (3) '….(a) identify the risks faced by the reporting entity in the ordinary course of its business, and
>
> (b) describe how the reporting entity will ensure that the assessment remains current; and
>
> (c) enable the reporting entity to determine the level of risk involved in relation to the relevant obligations under the Act and its regulations.

A reporting entity's risk assessment will be specific to it, and each of the above factors must be considered in relation to the particular attributes of the reporting entity.

In addition, when preparing a risk assessment, a reporting entity **must** consider any guidance material produced by the DIA supervisor or the Finance Intelligence Unit (FIU). Before undertaking a risk assessment, the following are key documents to have regard to:

- The National Risk Assessment (NRA) and FIU guidance material (accessible to reporting entities registered with the FIU's goAML system)[2]
- Sector risk assessments (SRAs) produced by the AML/CFT supervisors[3]
- Industry-specific guidance – for example, DIA has produced the Lawyers and Conveyancers Guideline[4].

After identifying and recording the risks, the reporting entity must assess the likelihood of each risk occurring and apply the risk assessment to its business through a compliance programme.

AML/CFT programme and Compliance Officer

Every reporting entity must have an AML/CFT programme that enables the reporting entity to detect money laundering and terrorism financing and manage and mitigate the risk of those activities occurring. The AML/CFT programme must be a dynamic document, e.g. one that is continually reviewed, edited and updated.

Every reporting entity must have a compliance officer. This person must be an employee of the business (refer to Appendix 1 - section 56, Part(2)). If there are no employees in the business, the reporting entity must appoint a person to act as the compliance officer. If the business is a partnership, a partner of the business may be appointed as the compliance officer and report to another partner.

The **AML Compliance Officer (AMLCO)** is responsible for administering the AML/CFT programme and training. They must report to a senior manager of the business. A senior manager is a director, or if not a company the equivalent role, such as a trustee or partner or someone with influence in the business such as a chief executive or chief financial officer.

The compliance programme should set out who the senior managers are in a business. An AMLCO can be shared among a Designated Business Group.

The AMLCO must also ensure they keep up-to-date with changes to methods and techniques (typologies) of money laundering and terrorism financing. The FIU provides relevant information and support with this.

[2] http://bit.ly/2zpmWPJ
[3] http://bit.ly/2HPNEou
[4] http://bit.ly/2GP2Bbi

Requirements for the AML/CFT programme and compliance officer are set out in **section 56** (refer to Appendix 1 – section 56) which states that a reporting entity must:

- Establish, implement, and maintain a written compliance programme
- Ensure the programme includes internal procedures, policies and controls to:
    - Detect money laundering and the financing of terrorism
    - Manage and mitigate the risk
    - Review and report on the risk assessment and compliance programme
- Designate an employee as an AML/CFT Compliance Officer (AMLCO)
    - Administer and maintain the compliance programme

Full details of the minimum requirements for AML/CFT programmes are set out in **section 57** of the AML/CFT Act (refer to Appendix 1 – section 57).

Note

The AML/CFT programme must be in writing and based on the risk assessment previously undertaken and include adequate and effective procedures, policies and controls for:

- Vetting certain personnel including senior managers, AML/CFT compliance officers and any other employees doing AML/CFT related duties
- Training for all who are engaged in AML/CFT activities including senior managers and the AMLCO
- Complying with customer due diligence requirements such as determining when enhanced customer due diligence must be done and when simplified customer due diligence may be permitted
- Reporting requirements for suspicious activity and prescribed transactions
- Record keeping requirements
- Ongoing systems to continually manage and mitigate the risks of money laundering and financing of terrorism
- Keeping and examining written findings in relation to transactions
- Keeping, examining and monitoring written findings in relation to business relationships and transactions from/to other countries

What does this mean for Licensees?

Every licensee **must** know and understand the AML/CFT programme and the role they play in ensuring their agency is operating in accordance with the programme and the Act.

Every licensee **must** know who their compliance officer (AMLCO), what their role is, why it is important and how to contact them.

Note

Every agent licensee **should** check with their insurer that they have sufficient professional indemnity cover for protection against exposure to AML/CFT breaches.

This is not only important for the agent licensee, but also for the designated AMLCO and all other licensees within the agency.

Complete the following details of your AML COMPLIANCE OFFICER (AMLCO) here: Name: Contact details:

Record keeping requirements

AML/CFT Act Section 49 covers the obligation to keep transaction records.

Key issue

The key issue to remember with record keeping is the ability to reconstruct the transaction after the fact.

Refer to Appendix 1 - section 49 Part (1), which states:

49 Obligation to keep transaction records

(1) In relation to every transaction that is conducted through a reporting entity, the reporting entity must keep those records that are reasonably necessary to enable that transaction to be readily reconstructed at any time.

In addition to transaction records, reporting entities must keep:

- Suspicious activity reports
- Identity and verification records
- Records that show the establishment of the business relationship, for example the agency agreement
- Records relating to the risk assessment and compliance programme

The DIA Guidelines December 2018 sets out specific requirements for retention of records. https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines#Real-Estate

These are as follows (refer to page 19 of DIA Guideline and Endnotes at the back of the guideline for associated footnotes: #39, #40 and #42):

Record type	Retention period
Transaction (as defined in the AML/CFT Act) records sufficient to enable the transactions to be fully reconstructed at any time[41]	5 years from the completion of the transaction
Any reports of suspicious activities[40]	5 years after the report is made
Identity and verification evidence (as reasonably necessary to enable the nature of the evidence to be readily identified at any time)[41]	5 years from the end of the business relationship or the completion of the occasional transaction or activity
Risk assessments, AML/CFT programmes and audits	5 years after the date on which they cease to be used on a regular basis
Information relevant to the establishment of a business relationship and any other records that explain the nature and purpose of a business relationship and the activities relating to that business relationship[42]	5 years from the end of the business relationship

Auditing

Reporting entities must ensure their risk assessment and AML/CFT programme are audited every two years, unless a different time period is prescribed according to section 59 of the AML/CFT Act.

This must be carried out by an independent person appointed by the reporting entity who is appropriately qualified (refer to Appendix 1 - section 59B). Furthermore, the auditor must not have been involved in the establishment, implementation or maintenance of the AML/CFT programme, or in undertaking the risk assessment.

Real estate agents are required to complete their first audit prior to 1 January 2021, i.e. two years from the date real estate agents were established as reporting entities (1 January 2019).

Annual Reporting

The reporting entity is also required to prepare an annual report on its risk assessment and AML/CFT programme (refer to AML/CFT Act section 60). This must be completed in the prescribed form and is to be submitted to their relevant supervisor between 1 July and 31 August each year.

Real estate agents will be required to submit their first annual report to the DIA at the end of August 2019 which will cover a six-month period (i.e. 1 January 2019 to 30 June 2019).

Note

A reporting entity must make available its risk assessment, AML/CFT compliance programme, audit reports and associated documents to the DIA at any time on request.

Reporting entities that have branches and subsidiaries must ensure that the branches and subsidies comply with the AML/CFT requirements relating to customer due diligence, risk assessments, AML/CFT compliance programme and record keeping (refer to Appendix 1 -AML/CFT Act section 61)

If a branch or subsidiary is in a country that does not permit carrying out AML/CFT requirements, the reporting entity must inform the DIA and take additional steps to manage the AML/CFT risks.

Questions:

Read the following statements and decide whether they are true or false.

8. The Risk Assessment **must** be in writing.

   True / False

9. The AML/CFT programme **must** be in writing.

   True / False

10. As part of its compliance programme a reporting entity must vet senior managers, compliance officers and all staff that are engaged in AML-CFT related duties.

    True / False

11. The key issue to remember regarding record keeping is the ability to reconstruct the transaction after the fact and to provide your rationale.

    True / False

12. Reporting entities are required to engage an auditor and ensure an audit of their risk assessment and AML/CFT programme is conducted *annually.*

    True / False

Undertaking due diligence: your obligations

The AML/CFT Act requires customer due diligence (CDD) to be carried out by a reporting entity on their customer.

Under the **Real Estate Agents Act 2008** and its regulations and rules, we use the terms:

> *client* to describe the person on whose behalf we carry out real estate agency work (see s 4 Real Estate Agents Act 2008), and
>
> *customer* to describe the person who is a party or potential party to a transaction but not a prospective client and a client (see **Real Estate Agents Act (Professional Conduct and Client Care) Rules 2012)**

Under the Real Estate Agents Act, a client is the person a real estate agency enters into an agency agreement with.

In contrast, the **AML/CFT Act 2009** uses the term **customer** to describe the person who a licensee is working on behalf of i.e. who the agency agreement or business relationship is with.

We need to clarify who our 'customer' is in terms of complying with the AML/CFT Act and carrying out CDD.

Who is our customer under the AML/CFT Act?

The real estate *client* is our AML/CFT *customer*

The Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2018 provides clarity of the definition of customer (as it applies to real estate) in section 5B, as follows:

5B Definition of customer

For the purposes of paragraph (c) of the definition of customer in section 5(1) of the Act, a customer, in relation to a real estate agent (as defined in section 4(1) of the Real Estate Agents Act 2008)—

(a) **means a client** (as defined in section 4(1) of the Real Estate Agents Act 2008) **of that real estate agent**; and

(b) does not include any party to a real estate transaction on whose behalf the real estate agent is not carrying out real estate agency work; but

(c) despite paragraph (b), includes a person who conducts an occasional transaction[5] with a real estate agent.

Therefore, real estate agents are required to carry out CDD on their **client – the person(s) who an agent carries out real estate agency work for and on behalf of, and who is in an agency relationship with the agent.**

The **client** (as referred to in the Real Estate Agent Act 2008)

IS

The **customer** (as referred to in the AML/CFT Act 2009)

So, the **customer** that CDD must be carried out on (according to AML/CFT requirements) is the **party you are entering into an agency agreement with** (the client).

The customer will generally be the vendor, but CDD is also required on a buyer when:

1. A SAR is filed on a buyer
2. $10,000 or more in cash is deposited into the agency's trust account
3. A deposit is refunded
4. A buyer's agency agreement is entered into.

[5] We will cover conducting CDD on a person in relation to an occasional transaction in the section on Occasional customers that follows

Customer Due Diligence

One of the key aspects of the AML/CFT Act that applies to all licensees is knowledge, understanding and compliance with customer due diligence (CDD) requirements.

A licensee must know who their *customer* is.

AML/CFT Act, Section 11 – Customer due diligence, Parts (1) & (2) (refer to Appendix 2) sets out the obligations and requirements for reporting entities to conduct customer due diligence on:

- A customer (i.e. real estate *client*) – *vendor/lessor or purchaser*
- Any **beneficial owner*** of a customer
- Any **person acting on behalf**** of a customer – power of attorney

To fully understand how due diligence applies within a real estate transaction, we will first look at each of the categories set out in section 11(1) & (2), as interpreted within **AML/CFT Act, Section 5 interpretation.**

customer—

(a) means a new customer or an existing customer; and

(b) includes—

(i) a facility holder:

(ii) a person conducting or seeking to conduct an occasional transaction or activity through a reporting entity:

(iii) a junket organiser as defined in section 4(1) of the Gambling Act 2003:

(iv) a person or class of persons declared by regulations to be a customer for the purposes of this Act; but

(c) excludes a person or class of persons that is declared by regulations not to be a customer for the purposes of this Act

An **existing customer** means – a customer who is in a business relationship[6] prior to the AML/CFT Act applying to the reporting entity.

A **facility holder** - has an account or arrangement that is provided by the reporting entity.

A **transaction** (according to section 5) – means any deposit, withdrawal, exchange, or transfer of funds (in any dominated currency), whether in cash; or by cheque, payment order, or other instruments; or by electronic or other non-physical means.

beneficial owner* means the individual who—

(a) has effective control of a customer or person on whose behalf a transaction is conducted; or

(b) owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted

[6] Business relationship in terms of real estate means - a signed agency agreement is in place

The term ***person acting on behalf***** is a common law concept, which is integral to the real estate industry as an agent acting on behalf of the principal to bring about a transaction. Other examples of acting on behalf of someone include –

- A trustee acting on behalf of a trust
- Power of attorney (assignee) acting on behalf of the assignor
- Executor acting on behalf of an estate
- A director acting on behalf of a company

Refer to DIA Guideline (below and page 23 of the December 2018 version, and the Endnotes at the back of the document for footnote #66)

You must also complete CDD on:	For example:
Any beneficial owner[66] of a client	Someone who owns more than 25 percent of a company that is your client* Someone who has effective control of a company that is your client
Any person acting on behalf of a client	A person exercising a power of attorney for your client A legal guardian acting on behalf of a minor who is your client An employee who has the authority to act on behalf of a company that is your client

Source: DIA Guideline: December 2018

https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines#Real-Estate

You must also complete CDD on:

- An existing customer, or
- Anyone who conducts *occasional activity* or an *occasional transaction* with you.

Existing customer (existing client)

The AML/CFT Act defines an existing customer as:

> 'a person who was [actively[7]] in a business relationship with a reporting entity immediately before the Act began applying to the reporting entity'.

CDD must be carried out on an existing customer if there has been a *material change* in the nature or purpose of the business relationship, and you have insufficient information about that customer (client).

The DIA states a *material change* as:

> '….an event, activity or situation that you identify that could change the level of ML/TF risk you may encounter'.

Occasional customers

According to the DIA, real estate agents are 'not required to carry out CDD on a person that is not your customer, other than in certain circumstances.'

An *occasional customer* is where a person carries out an *occasional activity*, or an *occasional transaction* where no business relationship has been established (refer to Appendix 3).

As noted in the DIA Guideline (refer to page 23, December 2018 version)

> 'When a person conducts an occasional activity or occasional transaction through your real estate business, that activity is covered by the AML/CFT Act.
>
> The person becomes a customer of yours, even though you do not have an agency agreement with them.
>
> As a licensee, you must comply with the requirements of the Act (including submitting SARs) in relation to that person.
>
> These requirements are additional to your CDD obligations relating to the customer that you have a business relationship with.'

Therefore, CDD must also be carried out on individuals that conduct an occasional activity or occasional transaction through a real estate agency.

A situation where an occasional transaction may occur is provided in the DIA Guideline as follows:

> 'If you receive funds from a party to a real estate transaction that is not your customer (i.e. is not the person you have an agency agreement with) of NZ$10,000 or more in cash (e.g. physical cash or cheque).'

[7] Any client that is currently in an agency agreement with the agent as of 1 January 2019

Example of the occasional transaction from DIA Guideline December 2018

When selling a house for a [real estate] client (who signs an agency agreement with you), you must comply with the requirements of the Act in relation to that client. In addition, if the purchaser of the house pays you funds (whether as a deposit or a settlement payment) of NZ$10,000 or more in physical cash or by cheque, you must also comply with the Act in relation to the purchaser (who is conducting an occasional transaction with you).

Customer due diligence levels

AML/CFT Act, Section 11 Part (3) (refer to Appendix 2) sets out three levels of customer due diligence required to be conducted, based on prescribed circumstances. These are:

- Standard customer due diligence (refer section 14 – Appendix 2)
- Simplified customer due diligence (refer section 18 – Appendix 2)
- Enhanced customer due diligence (refer section 22 – Appendix 2)

Note

Section 11 Part (4) states that once you have undertaken a CDD in accordance with the AML/CFT Act, you are NOT required to carry out another CDD (obtain or verify documents, data, or information previously obtained) UNLESS there are reasonable grounds to doubt the 'adequacy or veracity' of the information.

This means a licensee will not be required to undertake another CDD on a repeat customer unless you have reasons to doubt the adequacy or veracity of the information previously obtained. For example, where there has been a material change in the nature or purpose of the business relationship, and you have insufficient information about that customer (client).

Questions:

Read the following statements and decide whether they are true or false.

13. A customer as defined in section 5(1) of the AML/CFT Act means the client as defined in section 4(1) of the Real Estate Agents Act.

    True / False

14. An existing customer means – a customer who is in a business relationship prior to the AML/CFT Act applying to the reporting entity

    True / False

15. Customer Due Diligence is specified under two categories:
    - Standard customer due diligence (refer section 14)
    - Enhanced customer due diligence (refer section 22)

    True / False

16. A licensee will **not** be required to undertake another CDD on a 'repeat' customer **unless** you have reasons to doubt the adequacy or veracity of the information previously obtained, or if their identification has expired.

    True / False

Levels of customer due diligence

Standard customer due diligence

According to the DIA:

> 'Standard customer due diligence will apply to most residential and commercial property transactions in New Zealand'.

Standard customer due diligence (refer to Appendix 2, section 14) is required:

- If the reporting entity establishes a business relationship with a new customer
- If a customer seeks to conduct an occasional transaction or activity through the reporting entity
- If, in relation to an existing customer, and according to the level of risk involved, there has been a material change in the nature or purpose of the business relationship; and the reporting entity considers that it has insufficient information about the customer.

In addition to the above, as soon as a reporting entity becomes aware that an existing account is anonymous, standard customer due diligence must be conducted on that account.

Furthermore, regulations may be made in future that set out other circumstances when standard customer due diligence must be conducted.

Identity & verification requirements

Section 15 Standard customer due diligence; identity requirements, states that a reporting entity is required to obtain the following information:

> A reporting entity must obtain the following **identity** information in relation to the persons referred to in section 11(1) [as noted above]:
>
> (a) the person's full name; and
>
> (b) the person's date of birth; and
>
> (c) if the person is not the customer, the person's relationship to the customer; and
>
> (d) the person's address or registered office; and
>
> (e) the person's company identifier or registration number

You are also required to obtain 'information about the nature and purpose of the proposed business relationship with the customer, and sufficient information to determine whether enhanced CDD needs to be conducted on the customer' (refer section 17).

In addition to the identity requirements stated within section 15, the reporting entity is required to carry out verification of identity, as set out in section 16, which states:

Section 16 Standard customer due diligence; **verification of identity requirements**

(1) A reporting entity must—

(a) take reasonable steps to satisfy itself that the information obtained under section 15 is **correct**; and

(b) according to the level of risk involved, take reasonable steps to **verify any beneficial owner's identity** so that the reporting entity is satisfied that it knows who the beneficial owner is; and

(c) if a person is acting on behalf of the customer, according to the level of risk involved, take reasonable steps to **verify the person's identity and authority to act on behalf of the customer** so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer; and

(d) verify any other information prescribed by regulations.

The reporting entity **must** take reasonable steps to carry out verification of the identity information gathered **before** establishing a business relationship or conducting an occasional transaction or activity (refer to section 16(2))**.**

Section 16(3) provides an option for verification to be completed after the business relationship has been established:

(3) Verification of identity may be completed after the business relationship has been established if—

(a) it is essential not to interrupt normal business practice; and

(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and

(c) verification of identity is completed as soon as is practicable once the business relationship has been established.

Note: this delay is **only** in relation to the business relationship, and **not** in relation to the transaction.

Verification **must** be completed as soon as is practicable; and must be actioned **prior** to any sale/lease agreement being entered into.

Timing of due diligence

Further clarity around the timing of due diligence has been addressed in the Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Amendment Regulations 2018 effective from 1 January 2019.

The insertion of section 24A into the principal regulations (i.e. the AML/CFT (Definition) Regulations 2011) states:

> **24A Time at which real estate agents must conduct customer due diligence**
>
> For the purpose of sections 14(3), 18(3A), and 22(6) of the Act, a real estate agent **must** conduct customer due diligence **before** the real estate agent enters into an agency agreement (within the meaning of section 4(1) of the Real Estate Agents Act 2008) with a customer.

It is clear from regulation 24A that due diligence must be completed **before** an agency agreement is entered into[8]. This includes the requirement to carry out verification.

Agents should be cautioned that only in very rare cases might it be appropriate to consider deferring completion of due diligence until after an agency agreement has been executed.

As noted in the DIA Guideline document (page 36, December 2018);

> '…instances of delaying the verification of client identity information should be rare. The reasons for delaying verification should be fact-based, justifiable and recorded.'

Summary of standard customer due diligence

- **Identity –** full name, date of birth, and, if not the customer – their relationship to the customer, their address or registered office, company identifier or registration number
- **Verification –** check the identity information is correct, including *beneficial owner* if applicable. For example - passport to verify name and date of birth; utility bill to verify address; check company registrar's office to verify company details/director(s) names
- **Additional information –** nature/purpose of business relationship of the customer; decide if enhanced customer due diligence is required

[8] 'enters into' – as stated in section 24A above. Furthermore, CDD conducted after the client has signed the agency agreement, but prior to the real estate agency signing the agency agreement is likely to comply with Regulation 24A. This is not really relevant to the AML discussion.

Simplified customer due diligence

According to the DIA

simplified customer due diligence might apply if:

- A local council engages you to sell one of their properties
- You are engaged to sell a property for a state-owned enterprise
- You are engaged by a publicly listed company

Simplified customer due diligence (section 18 (1) – refer Appendix 2) may be conducted by a reporting entity if:

- It establishes a business relationship with one of the customers specified in section 18(2) of the AML/CFT Act; or
- One of the customers specified in section 18 (2) conducts an occasional transaction or activity through the reporting entity; or
- A customer conducts a transaction or obtains a product or service specified in regulations through the reporting entity

The customers listed in section 18 (2) are primarily state sector government departments, or a company whose equity securities are publicly listed in New Zealand or on an overseas stock exchange that has sufficient disclosure requirements.

Examples highlighted by the DIA include:

- Government departments
- Local authorities
- New Zealand Police
- State-owned enterprises
- Crown entities
- Registered banks

When engaged by a customer as noted above, you are required to record the full name of the entity and include a brief explanation of how it falls under section 18(2).

Simplified due diligence can also be conducted on a person *acting on behalf of* an existing customer, if standard or enhanced CDD has been done on that customer (Refer to AML/CFT Act, section 18 Part(3)).

Identity & verification requirements

The relevant identity requirements of the person acting on behalf of the entity when undertaking a simplified customer due diligence are set out in section 19 and include:

19 Simplified customer due diligence: identity requirements

A reporting entity must obtain the following identity information in relation to a person acting on behalf of the customer:

(a) the person's full name; and

(b) the person's date of birth; and

(c) the person's relationship to the customer

You are also required to obtain information about the nature and purpose of the proposed business relationship between you and your customer.

You must take reasonable steps to verify the identity of a person acting on behalf of a customer and their authority to act (refer section 20 – Appendix 2).

You do not have to identify or verify the identity of a beneficial owner of a customer for whom you have conducted simplified customer due diligence.

Remember regulation 24A states that due diligence must be completed before an agency agreement is entered into. This includes the requirement to carry out verification.

Simplified customer due diligence – Summary

- **Identity –** full name, date of birth, their relationship to the customer, anything further required under the regulations
- **Verification –** check the identity information is correct (e.g. passport to verify name/date of birth; utility bill to verify address; check company registrar's office to verify company details/director(s) names); verification must be carried out before the business relationship is established or the occasional transaction or activity is conducted; identity and verification of the identity of a beneficial owner of the customer is not necessary.
- **Additional information –** nature/purpose of business relationship of customer

Enhanced customer due diligence

Enhanced customer due diligence (refer section 22) applies if:

- The reporting entity establishes a business relationship with a customer, and/or if a customer seeks to conduct an occasional transaction or activity through the reporting entity, and that customer is:
    - a trust or another vehicle for holding personal assets
    - a non-New Zealand resident from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place
    - a company with nominee shareholders[9] or shares in bearer form[10]
- The customer seeks to conduct a complex, unusually large transaction or an unusual pattern of transactions that have no apparent or visible economic or lawful purpose
- When a reporting entity considers that the level of risk warrants an enhanced CDD

The DIA also requires an enhanced CDD to be carried out when you have cause to submit a suspicious activity report to the FIU.

It is essential that information about your customer's source of wealth or source of funds is obtained, recorded and verified when carrying out an enhanced CDD.

Additional care should be given where a customer's source of funds or wealth has come from their beneficial owner(s).

Identity & verification requirements

The identity requirements for enhanced CDD include:

a. the person's full name; and
b. the person's date of birth; and
c. if the person is not the customer, the person's relationship to the customer; and
d. the person's address[11] or registered office; and
e. the person's company identifier or registration number; and
f. any information prescribed by regulations

[9] Nominee shareholder means a person who holds shares on behalf of the actual owner (beneficial owner)
[10] Bearer form means a security that is not registered to an owner
[11] **Note**: A Trust is not an independent legal entity. As such, they are not required to have a physical address. However, Agents must ensure they obtain the physical address of at ALL trustees.

AML/CFT Act Section 23 (refer to Appendix 2) states the reporting entity must obtain:

- information relating to the source of funds; or wealth of the customer
- if a trust, the name and date of birth of each beneficiary of the trust
- if a discretionary trust or charitable trust or a trust with more than 10 beneficiaries, a description of
    - each class or type of beneficiary
    - if a charitable trust, the objects of the trust

Furthermore, the reporting entity must take reasonable steps to ensure information gathered is correct and carry out verification of any beneficial owner's identity. You must also take reasonable steps to verify the person's identity and authority to act on behalf of the customer so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer.

The reporting entity must carry out verification of identity before establishing a business relationship or conducting an occasional transaction or activity. However, section 24(3) outlines verification may be completed after the business relationship has been established if:

(a) it is essential not to interrupt normal business practice; and

(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and

(c) verification of identity is completed as soon as is practicable once the business relationship has been established

(refer to section 24 – Appendix 2).

Remember, AML/CFT Act regulation 24A states that due diligence **must** be completed before an agency agreement is entered into.

24A Time at which real estate agents must conduct customer due diligence

For the purpose of sections 14(3), 18(3A), and 22(6) of the Act, a real estate agent must conduct customer due diligence before the real estate agent enters into an agency agreement (within the meaning of section 4(1) of the Real Estate Agents Act 2008) with a customer.

This includes the requirement to carry out verification. Agents should be cautioned that only in *very rare cases* might it be appropriate to consider deferring completion of due diligence until after an agency agreement has been executed (refer page 36 of the DIA guidance, December 2018).

The reporting entity must also obtain information on the nature and purpose of the proposed business relationship between the customer and the reporting entity (refer section 25 – Appendix 2).

Additional enhanced CDD requirements

The AML/CFT Act sets additional requirements where enhanced CDD must be conducted. These are set out in section 22 and correspond to the following:

- Section 22(2): politically exposed person (PEP) (refer section 26 – Appendix 2)
- Section 22(3): wire transfers (refer sections 27 & 28 – Appendix 2)
- Section 22(4): use of new or developing technologies

You must conduct an enhanced CDD when:

- You determine that your customer is a PEP
- You are an ordering institution[12], an intermediary institution, or a beneficiary institution in relation to a wire transfer
- You are 'undertaking an activity that involves the use of new or developing technologies that may favour anonymity'
- Your customer is a trust

Licensees should refer all queries about enhanced CDD to their AMLCO to ensure compliance.

[12] **ordering institution**—
(a) means any person who has been instructed by a person (the **payer**) to electronically transfer funds controlled by the payer to a person (the **payee**) who may or may not be the payer on the basis that the transferred funds will be made available to the payee by a beneficiary institution; and
(b) includes a person declared by regulations to be an ordering institution for the purposes of this Act; but
(c) excludes a person or class of persons declared by regulations not to be an ordering institution for the purposes of this Act

Enhanced customer due diligence – Summary

- **Identity –** full name, date of birth, if not the customer – their relationship to the customer, their address or registered office, company identifier or registration number, and information relating to the source of funds; or wealth of the customer
    - If a trust, the name and date of birth of each beneficiary of the trust
    - If a discretionary trust or charitable trust or a trust with more than 10 beneficiaries, a description of
        - each class or type of beneficiary
        - if a charitable trust, the objects of the trust
- **Verification –** check that identity information is correct, including 'beneficial owner' if applicable (e.g. passport to verify name/date of birth; utility bill to verify address; check company registrar's office to verify company details/director(s) names); verification must be carried out before the business relationship is established or the occasional transaction or activity is conducted
- **Additional information**
    - Nature or purpose of business relationship of the customer
    - Source of funds or source of wealth

Questions:

Read the following statements and decide whether they are true or false.

17. A The AML/CFT Act requires all reporting entities to undertake customer due diligence

    True / False

18. There are four categories of customer due diligence

    True / False

19. Simplified Customer Due Diligence applies primarily to state sector government departments, or a company whose equity securities are publicly listed in New Zealand or on an overseas stock exchange that has sufficient disclosure requirements

    True / False

20. When a reporting entity's customer is a trust, whether a discretionary trust or a charitable trust, an enhanced customer due diligence must be undertaken

    True / False

Steps to follow when assessing CDD requirements

The DIA has provided examples within their Guideline document.

Each example sets out the recommended steps that a licensee should follow in order to assess the appropriate level of CDD required.

These steps are as follows:

1. Identify which criteria your customer meets to decide the level of CDD you must do.

   Refer to your in-house AML/CFT programme to help with criteria assessment

2. Obtain information about the nature and purpose of the proposed business relationship

3. Identify all relevant persons who need to be identified e.g. individuals, trustees, company directors

4. Make a determination of the level of ML/TF risk involved

5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the **Amended Identity Verification Code of Practice 2013** [and the associated **Explanatory Note**][13] (refer Appendix 4). Also, verify the customer's source of wealth or source of funds if required

6. If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.

[13] Identity verification needs to be done by collecting and sighting documents, data, or information provided from a reliable source. You are required to keep records of this information. The Amended Identity Verification Code of Practice 2013 provides suggested best practice for anyone conducting name and date of birth identity verification on clients (that are natural persons) who have been assessed to be low to medium risk. The Amended Identity Verification Code of Practice 2013 should be read in tandem with the Explanatory Note.

Examples of CDD

These examples are reproduced from the DIA Guideline – December 2018

Example 1 – Standard CDD: residential

Simple residential sale – individual as client

Client	Residential property – vendor as client
Covered activity	Selling family home
Level of CDD required	Standard CDD
Steps to complete	**How this applies to the example**
1. Identify which criteria your client meets to decide the level of CDD you must do.	According to your AML/CFT programme, this client meets the criteria for standard CDD.
2. Obtain information about the nature and purpose of the proposed business relationship.	Your client is a natural person and a New Zealand resident selling their family home. Your client explains that they are selling their property to finance the purchase of a new larger house.
3. Identify all relevant persons who need to be identified.	The client is the owner of the house. There is no reason to believe the client is acting on behalf of any other person. Therefore, you treat the client as also being the sole beneficial owner.
4. Make a determination of the level of ML/TF risk involved.	You determine the client presents low ML/TF risk. This is based on the following: they are not a politically exposed person (PEP), no cash is involved, they are a New Zealand resident, they have a low-risk occupation, and their behaviour is entirely normal for the activity being undertaken.
5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice 2013. Also verify the client's source of wealth or source of funds if required.	You obtain and verify the identity of your client by sighting their current New Zealand passport. You obtain the client's address from a recent bank statement. You take clear copies of all relevant documents and date and sign them. There is no need to determine source of wealth or source of funds.
6. If the identity information and verification requirements are satisfied, then you can proceed with the client's instructions.	Having met the criteria of the Act, you proceed with the sale of the residential property.

Example 2 – Standard CDD: commercial

Commercial property sale – company as client

Client	Local company – not listed on stock exchange
Covered activity	Selling their business and premises
Level of CDD required	Standard CDD

Steps to complete	How this applies to the example
1. Identify which criteria your client meets to decide the level of CDD you must do.	The client is a local company with numerous owners. All are resident in New Zealand and no high-risk factors appear to be present. You deal directly with the CEO, who is in New Zealand. You decide to conduct standard CDD.
2. Obtain information about the nature and purpose of the proposed business relationship.	The local company wants to sell its existing commercial property and buy a bigger property to extend its ability to carry out its business. The company is relatively new and is expanding its product range.
3. Identify all relevant persons who need to be identified.	For this client, it is apparent that ownership is spread over a number of individuals, none of whom own more than 25 percent. In this case, because no individual owns more than 25 percent, there is no beneficial owner on the basis of shareholding. However, you will still need to consider whether there are beneficial owners based on having effective control. Understanding the management and governance structure of your client helps you establish that the CEO is the person with effective control of the client. This means that they are a beneficial owner. The CEO is also the person acting on behalf of the company.
4. Make a determination of the level of ML/TF risk involved.	Neither the company nor the CEO is associated with any high risk factors identified in your risk assessment. You determine that the company presents a low risk and requires standard CDD.
5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice 2013. Also verify the client's source of wealth or source of funds if required.	With standard CDD for companies, the information you require from your client is as follows: • Full legal name and trading name (if different) • Principal business address or registered office address • Company identifier or registration number Company structure and arrangements should be verified using documents, data or information issued by reliable and independent sources – for instance, company certificates, annual reports, internet searches on reputable directories, or a list of directors. For the CEO, you obtain and verify their name and date of birth by sighting their firearms licence (a primary form of photo identification). They also provide a utility bill to verify their address. You take clear copies of all relevant documents and date and sign them. There is no need to determine source of wealth or source of funds.
6. If the identity information and verification requirements are satisfied, then you can proceed with the client's instructions.	You proceed with the sale of the commercial property.

Example 3 – Simplified CDD: commercial

Client	New Zealand listed company
Covered activity	Selling commercial property
Level of CDD required	Simplified
Steps to complete	**How this applies to the example**
1. Identify which criteria your client meets to decide the level of CDD you must do.	According to your AML/CFT programme, this new client meets the criteria for simplified CDD as it is a company listed on the New Zealand stock exchange.
2. Obtain information about the nature and purpose of the proposed business relationship.	Your client is selling commercial property that is surplus to their needs as they down-size. Even though you are conducting simplified CDD you must still obtain information on the nature and purpose of the business relationship.
3. Identify all relevant persons who need to be identified.	The client is a New Zealand listed company. You do not need to identify or verify the identity of any beneficial owners of the company. You will need to identify the employee of the client that you are dealing with and their relationship to the client.
4. Make a determination of the level of ML/TF risk involved.	You determine that the client is low risk given they are a reputable listed company on the New Zealand stock exchange. In addition, they are not involved in any high risk activities or jurisdictions, and have not been subject to criminal or civil sanctions relating to ML/TF.
5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice 2013. Also verify the client's source of wealth or source of funds if required.	You do not need to identify or verify the identity of beneficial owners of the client as part of simplified CDD. You will still need the company's full legal name and should record how the company qualifies for simplified CDD. You are dealing with an employee of the company who is acting on behalf of the client. You need to obtain and verify their identity information and authority to act. You obtain the person's full name and date of birth by sighting their passport. You take clear copies and date all relevant documents. The employee provides a formal letter of authorisation on headed paper. You are satisfied that they have authority to act on behalf of the company. You take a clear copy of the formal letter and date and sign it. There is no need to determine source of wealth or source of funds.
6. If the identity information and verification requirements are satisfied, then you can proceed with the client's instructions.	Having met the criteria of the Act, you proceed with the sale of the property.

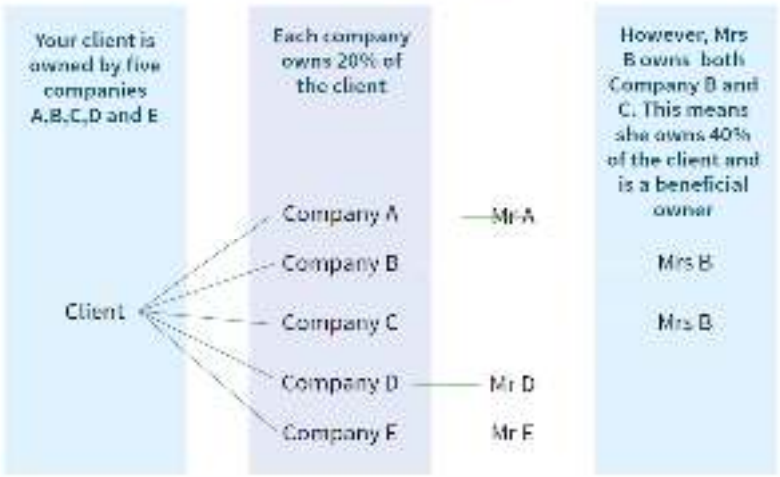
Example 4 – Enhanced CDD: family trust

Client	Residential vendor – family trust as client
Covered activity	Selling investment property
Level of CDD required	Enhanced CDD
Steps to complete	**How this applies to the example**
1. Identify which criteria your client meets to decide the level of CDD you must do.	According to your AML/CFT programme, this client meets the criteria for enhanced CDD as it is a trust.
2. Obtain information about the nature and purpose of the proposed business relationship.	Your client is a family trust selling an investment property. The trustee of the trust is the mother of the family. She is now retired and explains that the property is being sold to free up the equity it has accrued over the last ten years. This is to assist her two children, who are the beneficiaries.
3. Identify all relevant persons who need to be identified.	CDD will be required on the trust. You identify via the trust deed that there are two equal beneficiaries of the trust. As each beneficiary has an interest in over 25% of the trust property, each of them are beneficial owners and CDD must be conducted on them. You identify that the person you are dealing with, the mother, is the only trustee. You determine that she has effective control over the trust and is therefore also a beneficial owner. As this is a trust you are also required to examine its source of wealth or source of funds.
4. Make a determination of the level of ML/TF risk involved.	You determine the trust presents a low to medium level of ML/TF risk. This is based on the following: they are a trust, the beneficiaries are all New Zealand residents, the property has been in the trust for ten years, and the only other asset held by the trust is the family home. There are no PEPs involved, and there is only one family member with effective control over the client. Despite your low to medium risk rating, enhanced CDD is required by the Act. You conduct enhanced CDD according to the level of risk presented by the client.
5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice 2013. Also verify the client's source of wealth or source of funds if required.	The information required to identify the trust is: • Full name of the trust • Address of the trust • Name, date of birth and address of each beneficiary • Name, date of birth and address of the trustee • Source of wealth or source of funds of the trust You gather the information on the trust by sighting the original trust deed (of which you take a good quality copy and date and sign it). In relation to the trustee and the beneficiaries, you sight their current New Zealand driver licences and credit cards in their name to verify their names and birth dates. You also obtain and verify the address of the beneficiaries and trustee via provided bank statements. You take clear copies of all relevant documents and date and sign them. To verify the source of wealth or source of funds of the trust, you obtain other documents, including bank records and accounts audited by an accountant for the last three years. This shows that the investment property has been rented out to tenants, and that the trust has been paying tax on the income received.
6. If the identity information and verification requirements are satisfied, then you can proceed with the client's instructions.	Having met the criteria of the Act, you proceed with the sale of investment property.

Example 5 – Enhanced CDD: residential Politically Exposed Person (PEP)

Residential sale – PEP as client

Client	Overseas company
Covered activity	Selling investment property in New Zealand
Level of CDD required	Enhanced CDD

Steps to complete	How this applies to the example
1. Identify which criteria your client meets to decide the level of CDD you must do.	Your client is an overseas company from a higher-risk jurisdiction that is not listed on a stock exchange. They wish to sell their New Zealand based property. According to your AML/CFT programme, this client meets the criteria for enhanced CDD. Companies that are geographically or financially linked to higher-risk countries, or include PEPs, may have increased ML/TF risks.
2. Obtain information about the nature and purpose of the proposed business relationship. 3. Identify all relevant persons who need to be identified.	Your client is selling the New Zealand investment property to another company from the same high-risk jurisdiction. The client is owned by a number of other companies based in the same jurisdiction. Note: The information that you have gathered on the nature and purpose of the business relationship you will have with your client may also help determine the ML/TF risk that they may pose. Understanding the management and governance structure of your client will help you to establish the beneficial owners of your client. The company structure and arrangements should be verified using documents, data or information issued by reliable and independent sources – for instance, company certificates, annual reports, internet searches on reputable directories, or a list of directors. You determine that your client has the following beneficial ownership structure:  You must identify and verify the identity of all beneficial owners. The company has five direct owners, each owning an equal amount of the client. The beneficial owner threshold under the Act is someone who owns more than 25% of the client. Two of the five direct owners (Companies B and C) are wholly owned by Mrs B. As such, Mrs B is a beneficial owner of the client. As part of CDD you undertake a check on Mrs B to see if she is a PEP. This comes back positive as you identify that Mrs B was until recently a high ranking politician in the overseas jurisdiction. You deal directly with the New Zealand managing director of the company, Mr F. As well as acting on behalf of the company, you determine that Mr F also has effective control of the company. This means that you also need to conduct CDD on Mr F. **You do not have to conduct CDD on the company from the high-risk jurisdiction purchasing the property, as they are not your client.**

4. Make a determination of the level of ML/TF risk involved.	You determine the company presents a high level of ML/TF risk. This is based on the following: the beneficial owner is a PEP, the client has a complicated organisational structure, and the client is based in a high-risk jurisdiction. You are therefore required to conduct enhanced CDD.
5. Gather identity information and, according to the level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice 2013. Also verify the client's source of wealth or source of funds if required.	The information required for identification of the client is: • Full legal name • Trading name (if different) • Principal business address or registered office address • Jurisdiction of incorporation (optional) • Company identifier or registration number You must also examine the source of wealth or source of funds of the client. Their website and open source information indicate a long-running and reputable company. You request that the company provides you with the purchase agreement for the investment property and evidence of where the funds came from to make the purchase. You are provided with a certified copy of the purchase agreement, which shows it was bought three years ago. You are also provided with bank statements and accounts audited by an accountant that satisfy you that the investment property was purchased from legitimate sources. You also note that the contributions are proportional to their respective shareholdings. The information required for identification of the beneficial owner and person with authority to act are: • Name • Date of birth • Relationship to the client • Address The information you gather on Mrs B is in line with your enhanced CDD measures as detailed in your AML/CFT programme, including source of wealth or source of funds. A significant percentage of the client's funds appear to come from Mrs B. In this case the available information indicates that Mrs B was only in politics for a period of three years. Prior to that, she was a business person and also a person with family wealth who had accumulated business earnings and used it to buy and sell property. You are provided with certified copies of documents in accordance with the Amended Identity Verification Code of Practice 2013 confirming Mrs B's identity, as well as her address. In relation to Mrs B's source of wealth, you are provided with certified copies of her tax returns for the last five years. These records match your understanding of Mrs B's wealth and reflect a legitimate source of income. For Mr F you need to obtain and verify his identity and also his authority to act for the client. You obtain and verify his full name and date of birth by sighting his driver licence and credit card. You also sight his business card and carry out an internet search, which shows directories that list him as a contact for the company. You also obtain a formal letter of authorisation on headed paper provided by the client. You take clear copies of all relevant documents and date and sign them.
6. If the identity information and verification requirements are satisfied, then you can proceed with the client's instructions.	You are satisfied with the findings of your enhanced CDD. However, in line with the requirements of the Act, you have to escalate the decision to establish a business relationship with a PEP to your senior management. Your senior management team decide to establish the business relationship with the client but with instructions for regular ongoing CDD and activity monitoring in the event of more sales.

Reporting obligations under AML/CFT

As a licensee working with numerous customers as 'stewards of a real estate transaction', you are exposed to a vast array of people from all walks of life. We have looked in detail at the obligations of meeting CDD requirements. We will now look at your reporting obligations under the AML/CFT Act.

Financial Intelligence Unit (FIU)

We have discussed the role of the Department of Internal Affairs (DIA) as the *designated supervisor* for real estate agents as reporting entities.

The NZ Police Financial Intelligence Unit (FIU) hold another key role in Money Laundering / Financing Terrorism (ML/FT).

The FIU fulfils the functions and exercises powers of the Commissioner of Police as set out in the AML/CFT Act. It does this by providing financial intelligence relating to suspicious transactions/activity, money laundering, the financing of terrorism and other serious offences, which is achieved by collecting and collating information provided by external parties and reporting entities, banks and other financial institutions.

Source: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/about

As a reporting entity, real estate agents are required to submit reports via their AMLCO to the FIU about certain activities or transactions, as prescribed in the AML/CFT Act. These include:

- Suspicious activity reports (SARs), and
- Prescribed transaction reports (PTRs)

Each report is designed to help the FIU detect and deter ML/TF and could be the crucial piece of information that enables the FIU to take action against a criminal.

The FIU and DIA provide guidance and support to help reporting entities to identify suspicious activity and typical money laundering or terrorism financing *red flags* or indicators.

The FIU also provides help and support with queries. Refer to the following website link for more information:

http://www.police.govt.nz/advice/businesses-and-organisations/fiu

Suspicious activity reports (SARs)

Real estate agents are required to report suspicious activities from 1 January 2019 when the AML/CFT applies to them.

What is a suspicious activity?

AML/CFT Act Section 39A (refer to Appendix 5) defines suspicious activity as:

- an **activity** undertaken where:
    - a person **conducts or seeks to conduct a transaction** through a reporting entity, or
    - a reporting entity **provides or proposes to provide a service** to a person, or
    - a person **requests** a reporting entity **to provide a service or makes an enquiry** …in relation to a service; **and**
- the reporting entity has **reasonable grounds to suspect** that the **transaction or proposed transaction**…may be relevant to –
    - investigation of money laundering
    - breaches of law (Misuse of Drugs Act 1975; Terrorism Suppression Act 2002; Proceeds of Crime Act 1991 or Criminal Proceeds (Recovery) Act 2009;

So, SARs apply to:

- Transactions
- Proposed transactions
- Services
- Proposed services
- Inquiries

How do you know if something is suspicious?

As discussed at the beginning of this topic, typical money laundering activities include:

- Complex or unusually large transactions that are out of step with what you'd expect from the customer
- Unusual patterns of transactions or activity that have no apparent business or legal purpose
- Any other activity that appears to be related to criminal activity e.g. suspected terrorism, terrorism financing

A transaction may have many factors that, when considered individually, does not raise a suspicion, but, when considered collectively, suggests criminal activity. The challenge is making an objective judgement based on what might be deemed 'suspicious activity' and submitting the appropriate report.

What must be in a suspicious activity report?

Refer to AML/CFT Act Section 41 Nature of suspicious activity report (Appendix 5)

Reporting requirements

You **must** submit an SAR report 'as soon as practicable' after you have reasonable grounds for suspicion; and no later than 3 working days after you have gathered enough information to substantiate your suspicion. There are no monetary thresholds for SARs.

Key Point

It is important to note that you **must not disclose SAR information, or the existence of any SARs, to customers**

This is to protect the identity of staff and reporting entities who submit SARs and ensure their safety. It also avoids alerting the customer to the possibility of an investigation.

The DIA has stated that:

'It is not a defence that you did not actually consider an activity to be suspicious in circumstances where you objectively should have'.

Source: refer page 20, DIA Guidelines – August 2018; and page 20 for associated footnote reference #50; [2017] NZHC2363

http://www.nzlii.org/cgi-bin/sinodisp/nz/cases/NZHC/2017/2363.html?query=Ping%20An

Note: The FIU released a Suspicious Activity Reporting Guideline 2018:

http://www.police.govt.nz/sites/default/files/publications/suspicious-activity-reporting-guideline.pdf

Questions:

21. What transaction or activity may trigger the requirement to submit a SAR?

Tick all that apply.

a. Transactions
b. Services
c. Inquiries
d. Proposed transactions
e. Proposed services
f. Proposed enquiries that are suspicious

Prescribed transaction reports (PTRs)

From 1 January 2019, real estate agents are required to report certain prescribed transactions to the FIU.

The FIU explains a Prescribed Transaction Report (PTR) as a transaction conducted through a reporting entity in respect of:

- An **international wire transfer**[14] of NZD1,000 and over (also known as International Funds Transfers or IFTs) where at least one of the institutions (i.e. ordering, intermediary or beneficiary institution) involved in the transaction is **in** New Zealand, and at least one is **outside** New Zealand
- A **domestic physical cash transaction of NZD10,000 and over** (also known as Large Cash Transactions or LCTs) which are transactions in New Zealand involving the use of physical currency (i.e. coin and printed money designated as legal tender, and circulates as, and is customarily used and accepted as a medium of exchange in the country of issue).

Source: http://www.police.govt.nz/advice/businesses-and-organisations/financial-intelligence-unit-fiu/prescribed-transactions

Key Point

PTR reporting is designed to make it more difficult for criminals to use multiple small transactions, multiple senders or multiple recipients in order to avoid detection.

Wire transfers

Section 5 of the AML/CFT Act provides a definition of a wire transfer which, in summary, means transactions to transfer funds by electronic means (including instructions sent via the SWIFT network or by internet-based systems).

Note: the requirement to make a PTR is triggered by an international wire transfer of NZD1,000 or more; not a domestic wire transfer (refer to section 27(7)).

The FIU has provided a fact sheet regarding wire transfers: https://fma.govt.nz/assets/Fact-sheets/_versions/95/wire-transfers.1.pdf

Furthermore, **Section 27 – wire transfers: identity requirements** (refer to Appendix 1), sets out criteria for a reporting entity to comply with when identifying the originator of a wire transfer.

[14] **AML/CFT Wire Transfers Fact Sheet:**

Joint supervisory guidance from FMA, Reserve Bank and DIA:

https://fma.govt.nz/assets/Fact-sheets/_versions/95/wire-transfers.1.pdf

https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines?OpenDocument#WIR

Reporting requirements

You **must** submit a PTR report as soon as practicable after the transaction and no later than 10 working days after the transaction.

AML/CFT Act Section 48B sets out what must be in a PTR.

The prohibition on disclosing a SAR under sections 43-48 also apply to PTRs.

Note

As soon as a licensee becomes aware of any activity or transaction that requires either an SAR or PTR, they must contact their in-house AMLCO.

Suspicious Property Reports (SPRs)

The DIA Guideline -December 2018 also reminds licensees of your obligation to submit suspicious property reports (SPRs) under the Terrorism Suppression Act 2002 – refer to page 21 of the DIA Guideline.

goAML Web

SARs and PTRs must be submitted to FIU through goAML – Financial Intelligence Unit Reporting Tool. These reports must be submitted via goAML Web and must be actioned by the AMLCO on the prescribed form.

Real estate agents will need to register for 'goAML' to submit reports. Further information is available on the NZ Police website:

goAML – Financial Intelligence Unit reporting tool (external link)

Questions:

Read the following statements and decide whether they are true or false.

22. A Prescribed Transaction Report (PTR) is required if a licensee receives an international wire transfer over NZD1,000 in to the trust account.

True / False

23. If a licensee receives physical cash of less than NZD10,000 they must report this to the FIU as a Prescribed Transaction Report (PTR).

True / False

Reporting Summary

Reporting entities are required to make Suspicious Activity Reports (SARs) and Prescribed Transaction Reports (PTRs) on vendors and buyers.

As soon as a licensee becomes aware of any activity or transaction that requires either an SAR or PTR, they must contact their in-house AMLCO.

- Suspicious Activity Reports (SAR) must be submitted to the FIU through the online **form** in goAML:
  http://www.police.govt.nz/advice/financial-intelligence-unit-fiu/suspicious-activities-and-transactions-reports

- Prescribed Transaction Reports (PTRs) must be submitted to the FIU through the online **form** in goAML:

  http://www.police.govt.nz/advice/businesses-and-organisations/financial-intelligence-unit-fiu/prescribed-transactions

Relationships with other AML/CFT reporting entities

In recent times amendments to the AML/CFT Act have introduced significant changes for many businesses within New Zealand through increased monitoring and reporting requirements. More importantly, it has highlighted the significant exposure within New Zealand of extensive money laundering activities and the need for businesses to take their compliance obligations seriously.

It is important to remember that the real estate industry is not alone in this enhanced compliance regime. Banks and other financial institutions were initially captured under the AML Act under phase 1.

Other professions, including lawyers and accountants, have now been required to comply with the AML/CFT reporting and monitoring requirements under phase 2 along with real estate agents.

It is important to collaborate, wherever possible, with other reporting entities; namely, an interface between real estate agencies and lawyers (e.g. request from lawyers for assistance in alerting clients and customers of the need for AML/CFT due diligence requirements), accountants and banks, and other stakeholders in the real estate transaction.

Guidance on this topic can be found on the DIA website:

Guidance on 'related' for the formation of Designated Business Groups (DBGs) in relation to Designated Non-Financial Businesses (DNFBPs)

https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines#DBG-1

Recognising red flags

The DIA Guidelines – December 2018 document provides helpful information regarding *red flags*. We have highlighted some here, as follows:

Customer red flags (i.e. the real estate *client*)

- Entering into an agency agreement where:
    - the client is a business or a trust whose organisational structure is unusual or excessively complex
    - the client makes it difficult to identify the true beneficial owner or individual with effective control
    - the client is a shell company or company with bearer-shares
    - the client is reluctant to provide all relevant CDD information, or you have a reasonable doubt that the information provided is correct or sufficient
    - the client is a Politically Exposed Person (PEP)
    - there are unexpected activities compared to what you know about your client
    - the legal structure of the client is frequently altered, including name changes and transfers of ownership
- Entering into a conjunctional agency relationship – clarifying which reporting entity is required to undertake CDD
- Dealing with a client who is operating at a distance and wishes to enter into an agency agreement, e.g. resides elsewhere in New Zealand
- Dealing with a client who is residing outside New Zealand

Country or geographic red flags

- Countries with poor or insufficient AML/CFT measures
- Countries that have a high level of bribery and corruption
- Countries associated with tax evasion

Other red flags

- A property is bought and sold in quick succession
- The client is selling for less than the purchase or market price and/or is disinterested in obtaining a better price
- There is an unusual involvement of third parties
- Payments are received from un-associated or unknown third parties, and payments for fees are in cash where this would not be a typical method of payment

Expectations of the DIA on all licensees

The DIA expects real estate agents (and all licensees who are engaged or employed by an agent) to:

- Know your ML/TF risks
- Know what to expect from your AML/CFT supervisor
- Know how to apply the AML/CFT Act to your business
- Know how to apply the AML/CFT Act to your day-to-day real estate agency work
- Know your compliance requirements
- Know your *customer* (i.e. the real estate *client*)
- Know the ML/TF red flags
- Know where to get support, for example your AMLCO

Appendices

Appendix 1 – Excerpts from the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (known as the AML/CFT Act)

Section 3 – Purpose, Part 1

3 Purpose

(1) The purposes of this Act are—

(a) to detect and deter money laundering and the financing of terrorism; and

(b) to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and

(c) to contribute to public confidence in the financial system.

Section 4 – Overview, Part 3

4 Overview

(3) Part 2 deals with AML/CFT requirements and compliance and has 7 subparts, as follows:

(a) subpart 1 includes provisions dealing with requirements on reporting entities to **conduct due diligence** on customers and certain other persons, the ability of reporting entities to rely on third parties to carry out customer due diligence and other AML/CFT functions, and prohibitions on establishing or continuing business relationships and setting up facilities in certain circumstances:

(b) subpart 2 includes provisions dealing with requirements on reporting entities to **report suspicious activities** and protection of persons making suspicious activity reports:

(ba) subpart 2A sets out requirements on reporting entities to report certain prescribed transactions:

(c) subpart 3 sets out requirements on reporting entities to **keep records** and includes provisions concerning the storage and destruction of records:

(d) subpart 4 deals with reporting entities' internal policies and procedures relating to the prevention of money laundering and the financing of terrorism, including provisions setting out requirements for reporting entities to have **an AML/CFT programme** for detecting and managing the risk of money laundering and the financing of terrorism, to carry out a **risk assessment** before conducting customer due diligence or establishing an AML/CFT programme, and to review, audit, and report on their risk assessment and AML/CFT programmes:

(e) subpart 5 deals with codes of practice and includes provisions relating to the preparation of codes by AML/CFT supervisors, approval of codes of practice, and their legal effect:

(f) subpart 6 contains provisions relating to the reporting of certain movements of cash into and out of New Zealand.

Section 5 – Interpretation (part)

5 Interpretation

AML/CFT supervisor, in relation to a reporting entity, means the person referred to in section 130(1) that is responsible for supervising the reporting entity under Parts 3 and 4

beneficiary institution, in relation to a wire transfer from an ordering institution, means any person who receives those funds and then makes those funds available to a person (the payee) by—

(a) crediting it to an account held by the payee; or

(b) paying it to the payee

designated non-financial business or profession means –

(a) a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, a real estate agent, or a trust and company service provider, who, in the ordinary course of business, carries out 1 or more of the following activities: …

(v) providing real estate agency work (within the meaning of section 4(1) of the Real Estate Agents Act 2008) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008):…

prescribed transaction, in relation to a reporting entity, means a transaction conducted through the reporting entity in respect of—

(a) an international wire transfer of a value equal to or above the applicable threshold value; or

(b) a domestic physical cash transaction of a value equal to or above the applicable threshold value **prescribed transaction** report means a report made under section 48A

reporting entity

(a) means—
(i) a casino:
(ii) a designated non-financial business or profession:
(iii) a financial institution:
(iv) a high-value dealer:
(v) the New Zealand Racing Board; …

transaction—

(a) means any deposit, withdrawal, exchange, or transfer of funds (in any denominated currency), whether—
(i) in cash; or
(ii) by cheque, payment order, or other instrument; or
(iii) by electronic or other non-physical means; and

(b) without limiting paragraph (a), includes—
(i) any payment made in satisfaction, in whole or in part, of any contractual or other legal obligation; and
(ii) a transaction or class of transactions declared by regulations to be a transaction for the purposes of this Act; …

Section 27 – Wire transfers: identity requirements

27 Wire transfers: identity requirements

(1) A reporting entity that is an ordering institution must identify the originator of a wire transfer that is equal to or above the applicable threshold value by obtaining the following information:

(a) the originator's full name; and

(b) the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator; and

(c) one of the following:

(i) the originator's address:

(ii) the originator's national identity number:

(iii) the originator's customer identification number:

(iv) the originator's place and date of birth; and

(c) any information prescribed by section 27A or regulations.

(2) However, if the wire transfer is a domestic wire transfer, a reporting entity that is an ordering institution may identify the originator by obtaining the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator if the reporting entity that is the ordering institution is able to provide the information specified in subsection (1)(a), (c), and (d) within 3 working days of a request being made by the beneficiary institution.

(3) Regulations may be made under section 154(1)(c) exempting the reporting entity from the obligation to obtain some or all of the information set out in subsection (1) in relation to a specified transfer or transaction.

(4) The information obtained by the reporting entity (the ordering institution under subsection (1) or (2), as the case may be) must accompany the wire transfer.

(5) A reporting entity that is a beneficiary institution must—

(a) use effective risk-based procedures for handling wire transfers that are not accompanied by all the information specified in subsection (1); and

(b) consider whether the wire transfers constitute a suspicious activity.

(6) Any information about the originator obtained by a reporting entity that is an intermediary institution must be provided by that reporting entity to the beneficiary institution as soon as practicable.

(7) For the purposes of this section, a **domestic wire transfer** is a wire transfer where the ordering institution, the intermediary institution, and the beneficiary institution are all in New Zealand.

Section 49 – Obligation to keep transaction records

49 Obligation to keep transaction records

(1) In relation to every transaction that is conducted through a reporting entity, the reporting entity must keep those records that are reasonably necessary to enable that transaction to be readily reconstructed at any time.

(2) Without limiting subsection (1), records must contain the following information:

(a) the nature of the transaction**:**

(b) the amount of the transaction and the currency in which it was denominated:

(c) the date on which the transaction was conducted:

(d) the parties to the transaction:

(e) if applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by the reporting entity) directly involved in the transaction:

(f) the name of the officer or employee or agent of the reporting entity who handled the transaction, if that officer, employee, or agent—

(i) has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and

(ii) has formed a suspicion (of the kind referred to in section 40(1)(b)) about the transaction:

(g) any other information prescribed by regulations.

(3) A reporting entity must retain the records kept by that reporting entity, in accordance with this section, in relation to a transaction for—

(a) a period of at least 5 years after the completion of that transaction; or

(b) any longer period that the AML/CFT supervisor for the reporting entity, or the Commissioner, specifies.

Section 56 – Reporting entity must have AML/CFT programme and AML/CFT compliance officer

56 Reporting entity must have AML/CFT programme and AML/CFT compliance officer

(1) A reporting entity must establish, implement, and maintain a compliance programme (an AML/CFT programme) that includes internal procedures, policies, and controls to—

(a) detect money laundering and the financing of terrorism; and

(b) manage and mitigate the risk of money laundering and financing of terrorism.

(2) A reporting entity must designate an employee as an AML/CFT compliance officer to administer and maintain its AML/CFT programme.

(3) In the case of a reporting entity that does not have employees, the reporting entity must appoint a person to act as its AML/CFT compliance officer.

(4) The AML/CFT compliance officer must report to a senior manager of the reporting entity.

(5) Despite subsections (2) to (4), if a reporting entity is a partnership,—

(a) the partnership may designate one of the partners as an AML/CFT compliance officer to administer and maintain its AML/CFT programme, irrespective of whether the partnership has or does not have employees; and

(b) the partner so designated must report to another partner designated for the purpose of receiving those reports by the partnership.

Section 57 – Minimum requirements for AML/CFT programmes

57 Minimum requirements for AML/CFT programmes

(1) A reporting entity's AML/CFT programme must be in writing and be based on the risk assessment undertaken in accordance with section 58 and include adequate and effective procedures, policies, and controls for—

(a) vetting—

(i) senior managers:

(ii) the AML/CFT compliance officer:

(iii) any other employee that is engaged in AML/CFT related duties;

and

(b) training on AML/CFT matters for the following employees:

(i) senior managers:

(ii) the AML/CFT compliance officer:

(iii) any other employee that is engaged in AML/CFT related duties;

and

(c) complying with customer due diligence requirements (including ongoing customer due diligence and account monitoring); and

(d) reporting suspicious activities; and

(da) reporting prescribed transactions; and

(e) record keeping; and

(f) setting out what the reporting entity needs to do, or continue to do, to manage and mitigate the risks of money laundering and the financing of terrorism; and

(g) examining, and keeping written findings relating to,—

(i) complex or unusually large transactions; and

(ii) unusual patterns of transactions that have no apparent economic or visible lawful purpose; and

(iii) any other activity that the reporting entity regards as being particularly likely by its nature to be related to money laundering or the financing of terrorism; and

(h) monitoring, examining, and keeping written findings relating to business relationships and transactions from or in countries that do not have or have insufficient anti-money laundering or countering financing of terrorism systems in place and have additional measures for dealing with or restricting dealings with such countries; and

(i) preventing the use, for money laundering or the financing of terrorism, of products (for example, the misuse of technology) and transactions (for example, non-face-to-face business relationships or transactions) that might favour anonymity; and

(j) determining when enhanced customer due diligence is required and when simplified customer due diligence might be permitted; and

(k) providing when a person who is not the reporting entity may, and setting out the procedures for the person to, conduct the relevant customer due diligence on behalf of the reporting entity; and

(l) monitoring and managing compliance with, and the internal communication of and training in, those procedures, policies, and controls.

(2) In developing an AML/CFT programme, a reporting entity must have regard to any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to AML/CFT programmes.

Section 58 – Risk Assessment

58 Risk assessment

(1) Before conducting customer due diligence or establishing an AML/CFT programme, a reporting entity must first undertake an assessment of the risk of money laundering and the financing of terrorism (a risk assessment) that it may reasonably expect to face in the course of its business.

(2) In assessing the risk, the reporting entity must have regard to the following:

(a) the nature, size, and complexity of its business; and

(b) the products and services it offers; and

(c) the methods by which it delivers products and services to its customers; and

(d) the types of customers it deals with; and

(e) the countries it deals with; and

(f) the institutions it deals with; and

(g) any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to risk assessments; and

(h) any other factors that may be provided for in regulations.

(3) The risk assessment must be in writing and—

(a) identify the risks faced by the reporting entity in the course of its business; and

(b) describe how the reporting entity will ensure that the assessment remains current; and

(c) enable the reporting entity to determine the level of risk involved in relation to relevant obligations under this Act and regulations.

Section 59B – Who carries out audit

59BWho carries out audit

(1) An audit under section 59 or 59A must be carried out by an independent person, appointed by the reporting entity, who is appropriately qualified to conduct the audit.

(2) A person appointed to conduct an audit is not required to be—

(a) a chartered accountant within the meaning of section 19 of the New Zealand Institute of Chartered Accountants Act 1996; or

(b) qualified to undertake financial audits.

(3) A person appointed to conduct an audit must not have been involved in—

(a)the establishment, implementation, or maintenance of the reporting entity's AML/CFT programme (if any); or

(b) the undertaking of the reporting entity's risk assessment (if any).

(4) The audit of a risk assessment under section 59 is limited to an audit of whether the reporting entity's risk assessment fulfils the requirements in section 58(3).

(5) A reporting entity must provide a copy of any audit to its AML/CFT supervisor on request.

Section 61 – Reporting entities to ensure that branches and subsidiaries comply with AML/CFT requirements

61 Reporting entities to ensure that branches and subsidiaries comply with AML/CFT requirements

(1) A reporting entity must ensure that its branches and subsidiaries that are in a foreign country apply, to the extent permitted by the law of that country, measures broadly equivalent to those set out in this Act and regulations with regard to the requirements for customer due diligence (including ongoing customer due diligence), risk assessments, AML/CFT programmes, and record keeping.

(2) If the law of the foreign country does not permit the application of those equivalent measures by the branch or the subsidiary located in that country, the reporting entity must—

(a) inform its AML/CFT supervisor accordingly; and

(b) take additional measures to effectively handle the risk of a money laundering offence and the financing of terrorism.

(3) A reporting entity must communicate (where relevant) the policies, procedures, and controls that it establishes, implements, and maintains in accordance with this subpart to its branches and subsidiaries that are outside New Zealand.

Section 63 – AML/CFT supervisors to prepare codes of practice for relevant sectors (Parts 1 and 2)

63 AML/CFT supervisors to prepare codes of practice for relevant sectors

(1) An AML/CFT supervisor must, if directed to do so by the Minister responsible for that AML/CFT supervisor (the responsible Minister), prepare—

(a) 1 or more codes of practice for the sector of activity of the reporting entities for which it is the supervisor under section 130 or in respect of different reporting entities specified by the responsible Minister:

(b) an instrument that amends a code of practice or revokes the whole or any provision of a code of practice prepared under paragraph (a).

(2) The purpose of a code of practice is to provide a statement of practice that assists reporting entities to comply with their obligations under this Act and regulations…

Section 130 – AML/CFT supervisors (Parts 1 and 5)

130 AML/CFT supervisors

(1) The AML/CFT supervisors are as follows:

(a) for registered banks, life insurers, and non-bank deposit takers, the Reserve Bank of New Zealand (Reserve Bank) is the relevant AML/CFT supervisor:

(b) for persons referred to in subsection (1A) (other than banks, life insurers, and non-bank deposit takers), the Financial Markets Authority is the relevant AML/CFT supervisor:

(c) for designated non-financial businesses or professions and high-value dealers, the Department of Internal Affairs, or another AML/CFT supervisor prescribed for the purpose, is the relevant AML/CFT supervisor:

(d) for the New Zealand Racing Board, casinos, non-deposit-taking lenders, money changers, and other reporting entities that are not covered by paragraphs (a) to (c), the Department of Internal Affairs is the relevant AML/CFT supervisor…

…

(5) A reporting entity may have only 1 AML/CFT supervisor.

Section 131 - Functions

131 Functions

The functions of an AML/CFT supervisor are to—

(a) monitor and assess the level of risk of money laundering and the financing of terrorism across all of the reporting entities that it supervises:

(b) monitor the reporting entities that it supervises for compliance with this Act and regulations, and for this purpose to develop and implement a supervisory programme:

(c) provide guidance to the reporting entities it supervises in order to assist those entities to comply with this Act and regulations:

(d) investigate the reporting entities it supervises and enforce compliance with this Act and regulations:

(e) co-operate through the AML/CFT co-ordination committee (or any other mechanism that may be appropriate) with domestic and international counterparts to ensure the consistent, effective, and efficient implementation of this Act.

Section 132 – Powers (Parts 1 and part of Part 2)

132 Powers

(1) An AML/CFT supervisor has all the powers necessary to carry out its functions under this Act or regulations.

(2) Without limiting the power conferred by subsection (1), an AML/CFT supervisor may,—

(a) on notice, require production of, or access to, all records, documents, or information relevant to its supervision and monitoring of reporting entities for compliance with this Act; and

(b) conduct on-site inspections in accordance with section 133; and

(c) provide guidance to the reporting entities it supervises by—

(i) producing guidelines; and

(ii) preparing codes of practice in accordance with section 63; and

(iii) providing feedback on reporting entities' compliance with obligations under this Act and regulations; and

(iv) undertaking any other activities necessary for the assisting reporting entities to understand their obligations under this Act and regulations, including how best to achieve compliance with those obligations;…

Appendix 2 - AML/CFT Act: customer due diligence sections

Section 11 – Customer due diligence (Parts 1 to 4)

11 Customer due diligence

(1) A reporting entity must conduct customer due diligence on—

(a) a customer:

(b) any beneficial owner of a customer:

(c) any person acting on behalf of a customer.

(2) For the purposes of subsection (1)(b), a customer who is an individual and who the reporting entity believes on reasonable grounds is not acting on behalf of another person is to be treated as if he or she were also the beneficial owner unless the reporting entity has reasonable grounds to suspect that that customer is not the beneficial owner.

(3) The type of customer due diligence that must be conducted by a reporting entity is,—

(a) in the circumstances described in section 14, at least standard customer due diligence:

(b) in the circumstances described in section 18, at least simplified customer due diligence:

(c) in the circumstances described in section 22, enhanced customer due diligence.

(4) A reporting entity that is required to conduct customer due diligence in the circumstances described in sections 14, 18, and 22 is **not required** to obtain or verify any documents, data, or information that it has previously obtained and verified for the purposes of carrying out customer due diligence in accordance with this Act, unless there are reasonable grounds for the reporting entity to doubt the adequacy or veracity of the documents, data, or information previously obtained.

Section 14 – Circumstances when standard due diligence applies

14 Circumstances when standard customer due diligence applies

(1) A reporting entity must conduct standard customer due diligence in the following circumstances:

(a) if the reporting entity establishes a business relationship with a new customer:

(b) if a customer seeks to conduct an occasional transaction or activity through the reporting entity:

(c) if, in relation to an existing customer, and according to the level of risk involved,—

(i) there has been a material change in the nature or purpose of the business relationship; and

(ii) the reporting entity considers that it has insufficient information about the customer:

(d) any other circumstances specified in subsection (2) or in regulations.

(2) For the purposes of subsection (1)(d), as soon as practicable after a reporting entity becomes aware that an existing account is anonymous, the reporting entity must conduct standard customer due diligence in respect of that account.

(3) Despite subsections (1) and (2), a real estate agent must conduct standard customer due diligence at the times, and with any other modifications, specified in regulations.

Section 15 – Standard customer due diligence: identity requirements

15 Standard customer due diligence: identity requirements

A reporting entity must obtain the following identity information in relation to the persons referred to in section 11(1):

(a) the person's full name; and

(b) the person's date of birth; and

(c) if the person is not the customer, the person's relationship to the customer; and

(d) the person's address or registered office; and

(e) the person's company identifier or registration number; and

(f) any information prescribed by regulations.

Section 16 – Standard customer due diligence: verification of identity requirements (Parts 1 and 3)

16 Standard customer due diligence: verification of identity requirements

(1) A reporting entity must—

(a) take reasonable steps to satisfy itself that the information obtained under section 15 is correct; and

(b) according to the level of risk involved, take reasonable steps to verify any beneficial owner's identity so that the reporting entity is satisfied that it knows who the beneficial owner is; and

(c) if a person is acting on behalf of the customer, according to the level of risk involved, take reasonable steps to verify the person's identity and authority to act on behalf of the customer so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer; and

(d) verify any other information prescribed by regulations.

(2) Except as provided in subsection (3), a reporting entity must carry out verification of identity before establishing a business relationship or conducting an occasional transaction or activity.

(3) Verification of identity may be completed after the business relationship has been established if—

(a) it is essential not to interrupt normal business practice; and

(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and

(c) verification of identity is completed as soon as is practicable once the business relationship has been established.

Section 17 – Standard customer due diligence: other requirements

17 Standard customer due diligence: other requirements

A reporting entity must also obtain—

(a) information on the nature and purpose of the proposed business relationship between the customer and the reporting entity; and

(b) sufficient information to determine whether the customer should be subject to enhanced customer due diligence.

Section 18 – Circumstances when simplified customer due diligence applies

18 Circumstances when simplified customer due diligence applies

(1) A reporting entity may conduct simplified customer due diligence if—

(a) it establishes a business relationship with one of the customers specified in subsection (2); or

(b) one of the customers specified in subsection (2) conducts an occasional transaction or activity through the reporting entity; or

(c) a customer conducts a transaction or obtains a product or service specified in regulations through the reporting entity.

(2) The following are customers for the purposes of subsection (1):

(a) a listed issuer (within the meaning of section 6(1) of the Financial Markets Conduct Act 2013) that is the issuer of quoted voting products (within the meaning of that Act):

(b) a government department named in Schedule 1 of the State Sector Act 1988:

(c) a local authority, as defined in section 5(2) of the Local Government Act 2002:

(d) the New Zealand Police:

(e) a State enterprise (within the meaning of section 2 of the State-Owned Enterprises Act 1986) and a new State enterprise (as listed in Schedule 2 of that Act):

(f) a body that—

(i) corresponds to a State enterprise or a new State enterprise (as defined

in paragraph (e); and

(ii) is located in a country that has sufficient AML/CFT systems:

(g) *[Repealed]*

(h) a person licensed to be a supervisor or statutory supervisor under the Financial

Markets Supervisors Act 2011, when the person acts for itself:

(i) a trustee corporation, within the meaning of section 2(1) of the Administration Act 1969, when the trustee corporation acts for itself:

(j) a Crown entity, as defined in section 7(1) of the Crown Entities Act 2004:

(k) an organisation named in Schedule 4 of the Public Finance Act 1989:

(l) a company named in Schedule 4A of the Public Finance Act 1989:

(m) a government body that—

(i) corresponds to a government department named in Schedule 1 of the State Sector Act 1988; and

(ii) is located in an overseas jurisdiction that has sufficient AML/CFT systems:

(n) a registered bank within the meaning of section 2(1) of the Reserve Bank of New Zealand Act 1989:

(o) a licensed insurer within the meaning of section 6(1) of the Insurance (Prudential Supervision) Act 2010:

(p) a company, or a subsidiary (within the meaning of section 5(1) of the Companies Act 1993) of that company,—

(i) whose equity securities are listed in New Zealand or on an overseas stock exchange that has sufficient disclosure requirements;

and

(ii) that is located in a country that has sufficient AML/CFT systems in place:

(q) any other entity or class of entities specified in regulations.

(3) A reporting entity may also conduct simplified customer due diligence on a person who purports to act on behalf of a customer when—

(a) the reporting entity already has a business relationship with the customer at the time the person acts on behalf of the customer; and

(b) the reporting entity has conducted one of the specified types of customer due diligence on the customer in accordance with this Act and regulations (if any).

(3A) Despite subsections (1) to (3), a real estate agent must conduct simplified customer due diligence at the times, and with any other modifications, specified in regulations.

(4) For the avoidance of doubt, nothing in this subpart requires identification or verification of identity of a beneficial owner of a customer in respect of whom a reporting entity may conduct simplified customer due diligence.

Section 19 – Simplified customer due diligence: identity requirements

19 Simplified customer due diligence: identity requirements

A reporting entity must obtain the following identity information in relation to a person acting on behalf of the customer:

(a) the person's full name; and

(b) the person's date of birth; and

(c) the person's relationship to the customer; and

(d) any information prescribed by regulations.

Section 20 – Simplified customer due diligence: verification of identity requirements

20 Simplified customer due diligence: verification of identity requirements

(1) A reporting entity must, according to the level of risk involved, verify the identity of a person acting on behalf of a customer and that person's authority to act for the customer so that it is satisfied it knows who the person is and that the person has authority to act on behalf of the customer.

(2) Verification of identity must be carried out before the business relationship is established or the occasional transaction or activity is conducted or the person acts on behalf of the customer.

(3) For the purposes of verifying a person's authority to act in the circumstances described in section 18, a reporting entity may rely on an authority provided in an application form or other document provided to the reporting entity that shows a person's authority to act or transact on an account.

Section 22 – Circumstances when enhanced customer due diligence applies

22 Circumstances when enhanced customer due diligence applies

(1) A reporting entity must conduct enhanced customer due diligence in accordance with sections 23 and 24 in the following circumstances:

(a) if the reporting entity establishes a business relationship with a customer that is—

(i) a trust or another vehicle for holding personal assets:

(ii) a non-resident customer from a country that has insufficient antimony laundering and countering financing of terrorism systems or measures in place:

(iii) a company with nominee shareholders or shares in bearer form:

(b) if a customer seeks to conduct an occasional transaction or activity through the reporting entity and that customer is—

(i) a trust or another vehicle for holding personal assets:

(ii) a non-resident customer from a country that has insufficient antimony laundering and countering financing of terrorism systems or measures in place:

(iii) a company with nominee shareholders or shares in bearer form:

(c) if a customer seeks to conduct, through the reporting entity, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose:

(d) when a reporting entity considers that the level of risk involved is such that enhanced due diligence should apply to a particular situation:

(e) any other circumstances specified in section 22A or regulations.

(2) A reporting entity must conduct enhanced customer due diligence in accordance with section 26 if—

(a) it establishes a business relationship with a customer who it has determined is a politically exposed person; or

(b) a customer who it has determined is a politically exposed person seeks to conduct an occasional transaction or activity through the reporting entity.

(3) A reporting entity must conduct enhanced customer due diligence in accordance with sections 27 and 28 if it is an ordering institution, an intermediary institution, or a beneficiary institution in relation to a wire transfer.

(4) A reporting entity must conduct enhanced customer due diligence in accordance with section 29 if it has, or proposes to have, a correspondent banking relationship.

(5) A reporting entity must conduct enhanced due diligence in accordance with section 30 if—

(a) it establishes a business relationship with a customer that involves new or developing technologies, or new or developing products, that might

favour anonymity; or

(b) a customer seeks to conduct an occasional transaction or activity through the reporting entity that involves new or developing technologies, or new or developing products, that might favour anonymity.

(6) Despite subsections (1) to (5), a real estate agent must conduct enhanced customer due diligence at the times, in the circumstances, and with any other modifications specified in regulations.

Section 22A – Enhanced customer due diligence required for certain activities requiring suspicious activities report

22A Enhanced customer due diligence required for certain activities requiring suspicious activities report

(1) This section applies to an activity—

(a) that the reporting entity concerned (other than a high-value dealer) is required to report to the Commissioner under section 40; and

(b) that is not otherwise exempt from the customer due diligence requirements or from all the requirements of the Act; and

(c) that is conducted, or sought to be conducted,—

(i) by an existing customer; or

(ii) by a customer engaging in an occasional transaction or activity.

(2) For the purposes of section 22(1)(e), as soon as practicable after a reporting entity becomes aware that the reporting entity must report the suspicious activity under section 40, a circumstance occurs in which the reporting entity must conduct enhanced customer due diligence in respect of that activity.

Section 23 – Enhanced customer due diligence: identity requirements

23 Enhanced customer due diligence: identity requirements

(1) A reporting entity must, in relation to a person referred to in section 11(1), obtain the information required under section 15 and the following additional information:

(a) information relating to the source of the funds or the wealth of the customer;

and

(b) the additional information referred to in subsection (2) and any additional information prescribed by regulations.

(2) For the purposes of subsection (1)(b), a reporting entity must obtain,—

(a) in the case of a trust other than a trust to which paragraph (b) applies, the name and the date of birth of each beneficiary of the trust:

(b) in the case of a customer that is a discretionary trust or a charitable trust or a trust that has more than 10 beneficiaries, a description of—

(i) each class or type of beneficiary:

(ii) if the trust is a charitable trust, the objects of the trust.

Section 24 – Enhanced customer due diligence: verification of identity requirements

24 Enhanced customer due diligence: verification of identity requirements

(1) A reporting entity must—

(a) conduct the verification of identity requirements for standard customer due diligence set out in section 16; and

(b) according to the level of risk involved, take reasonable steps to verify the information obtained under section 23(1)(a); and

(c) verify any other information prescribed by regulations.

(2) Except as provided in subsection (3), a reporting entity must carry out verification of identity before establishing a business relationship or conducting an occasional transaction or activity.

(3) Verification of identity may be completed after the business relationship has been established if—

(a) it is essential not to interrupt normal business practice; and

(b) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and

(c) verification of identity is completed as soon as is practicable once the business relationship has been established.

Section 25 – Enhanced customer due diligence: other requirements

25 Enhanced customer due diligence: other requirements

In the circumstances described in section 22(1)(a), 22(2)(a), and 22(5)(a), a reporting entity must also obtain information on the nature and purpose of the proposed business relationship between the customer and the reporting entity.

Section 26 – Politically exposed person

26 Politically exposed person

(1) The reporting entity must, as soon as practicable after establishing a business relationship or conducting an occasional transaction or activity, take reasonable steps to determine whether the customer or any beneficial owner is a politically exposed person.

(2) If a reporting entity determines that a customer or beneficial owner with whom it has established a business relationship is a politically exposed person, then—

(a) the reporting entity must have senior management approval for continuing the business relationship; and

(b) the reporting entity must obtain information about the source of wealth or funds of the customer or beneficial owner and take reasonable steps to verify the source of that wealth or those funds.

(3) If a reporting entity determines that a customer or beneficial owner with whom it has conducted an occasional transaction or activity is a politically exposed person, then the reporting entity must, as soon as practicable after conducting that transaction or other activity, take reasonable steps to obtain information about the source of wealth or funds of the customer or beneficial owner and verify the source of that wealth or those funds.

Section 27 – Wire transfers: identity requirements

27 Wire transfers: identity requirements

(1) A reporting entity that is an ordering institution must identify the originator of a wire transfer that is equal to or above the applicable threshold value by obtaining the following information:

(a) the originator's full name; and

(b) the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator; and

(c) one of the following:

(i) the originator's address:

(ii) the originator's national identity number:

(iii) the originator's customer identification number:

(iv) the originator's place and date of birth; and

(d) any information prescribed by section 27A or regulations.

(2) However, if the wire transfer is a domestic wire transfer, a reporting entity that is an ordering institution may identify the originator by obtaining the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator if the reporting entity that is the ordering institution is able to provide the information specified in subsection (1)(a), (c), and (d) within 3 working days of a request being made by the beneficiary institution.

(3) Regulations may be made under section 154(1)(c) exempting the reporting entity from the obligation to obtain some or all of the information set out in subsection (1) in relation to a specified transfer or transaction.

(4) The information obtained by the reporting entity (the ordering institution under subsection (1) or (2), as the case may be) must accompany the wire transfer.

(5) A reporting entity that is a beneficiary institution must—

(a) use effective risk-based procedures for handling wire transfers that are not accompanied by all the information specified in subsection (1); and

(b) consider whether the wire transfers constitute a suspicious activity.

(6) Any information about the originator obtained by a reporting entity that is an intermediary institution must be provided by that reporting entity to the beneficiary institution as soon as practicable.

(7) For the purposes of this section, a **domestic wire transfer** is a wire transfer where the ordering institution, the intermediary institution, and the beneficiary institution are all in New Zealand.

Section 27A – Other identifying information prescribed in relation to wire transfers

27A Other identifying information prescribed in relation to wire transfers

(1) Information that gives the name of the beneficiary of a wire transfer and the account number of that beneficiary or any unique transaction reference that allows the transaction to be traced is prescribed for the purposes of section 27(1)(d).

(2) In the case of a domestic wire transfer, any information that enables the transaction itself to be identified and traced to the originator is prescribed to be other identifying information for the purposes of section 27(2).

Section 28 – Wire transfers: verification of identity requirements

28 Wire transfers: verification of identity requirements

(1) The ordering institution must, according to the level of risk involved,—

(a) verify the originator's identity so that the reporting entity is satisfied that the information obtained under section 27 is correct; and

(b) verify any other information prescribed by regulations.

(2) Verification of the originator's identity must be carried out before the wire transfer is ordered.

Appendix 3 - Occasional activity or transaction and definition of customer

Section 5 – Interpretation

occasional activity—

(a) means an activity—

(i) that is specified in section 6(4) in relation to a reporting entity (other than an occasional transaction); and

(ii) that does not involve a business relationship between the reporting entity and the reporting entity's customer; and

(b) includes an activity or a class of activities declared by regulations to be an occasional activity for the purposes of this Act; but

(c) excludes an activity or a class of activities declared by regulations not to be an occasional activity for the purposes of this Act

occasional transaction—

(a) means a cash transaction that occurs outside of a business relationship and is equal to or above the applicable threshold value (whether the transaction is carried out in a single operation or several operations that appear to be linked); and

(b) includes a transaction or class of transactions declared by regulations to be an occasional transaction for the purposes of this Act; but

(c) excludes—

(i) cheque deposits; and

(ii) a transaction or class of transactions declared by regulations not to

be an occasional transaction for the purposes of this Act

occasional transaction or activity means—

(a) an occasional transaction:

(b) an occasional activity

Section 5B – AML/CFT (Definitions) Amendment Regulations 2018

5B Definition of customer

For the purposes of paragraph (c) of the definition of customer in section 5(1) of the Act, a customer, **in relation to a real estate agent** (as defined in section 4(1) of the Real Estate Agents Act 2008)—

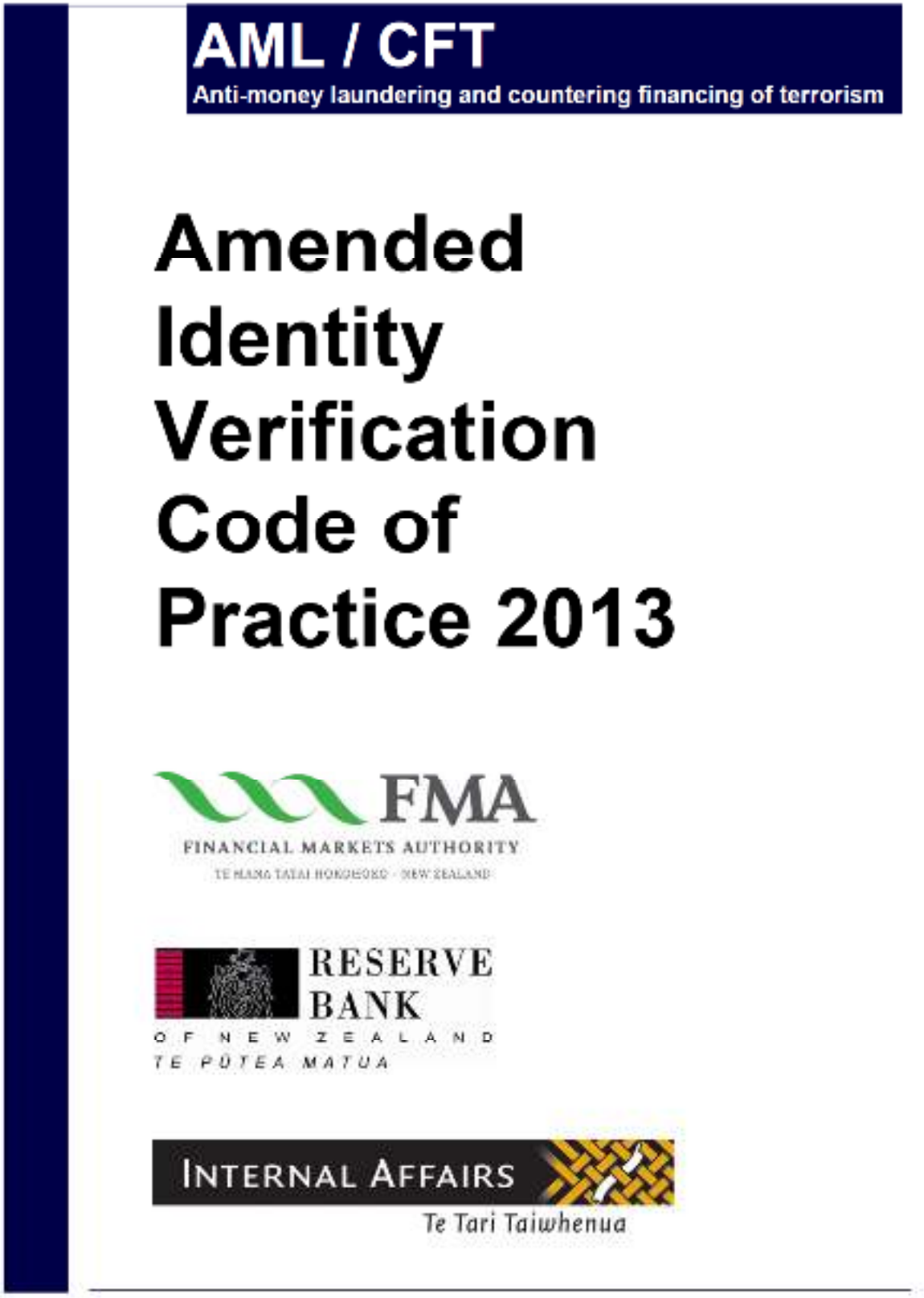
(a) means a client (as defined in section 4(1) of the Real Estate Agents Act 2008) of that real estate agent; and

(b) does not include any party to a real estate transaction on whose behalf the real estate agent is not carrying out real estate agency work; but

(c) despite paragraph (b), includes a person who conducts an occasional transaction with a real estate agent.

Appendix 4 - Identity Verification Code of Practice 2013 / Explanatory Note (Dec 2017)

https://fma.govt.nz/assets/Reports/_versions/3305/110901-identity-verification-code-of-practice-aml-cft-2011.2.pdf



Amended Identity Verification Code of Practice 2013

(Anti-Money Laundering and Countering Financing of Terrorism Act 2009 sections 16, 20, 24 and 28 for all reporting entities)

The Identity Verification Code of Practice (the code) was approved by notice in the New Zealand Gazette on the 1st day of September 2011 by the Ministers of Finance, Commerce and Internal Affairs under section 64 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act). This amended code of practice was approved by notice in the New Zealand Gazette on the 10th day of October 2013.

Introduction

The Identity Verification Code of Practice 2013 Explanatory Note provides background information and resources and should be read in conjunction with this code.

What is this code of practice for?
This code of practice provides a suggested best practice for all reporting entities conducting name and date of birth identity verification on customers (that are natural persons) that have been assessed to be low to medium risk. Identification involves obtaining from the customer a range of information about him or her ("identity information"). Verification involves confirming some of that information against documents, data or information obtained from a reliable and independent source.

Under section 11 of the AML/CFT Act a reporting entity must conduct customer due diligence on a customer; a beneficial owner of a customer; and any person acting on behalf of a customer. In this code of practice, *customer* refers to all natural persons that fall within these categories assessed by reporting entities as low to medium risk (that is falling within sections 11(1)(a) – (c)).

This code of practice provides for two ways of conducting identity verification, via documentary verification and electronic verification (Parts 1 and 3 of the code). Part 2 of the code provides for the certification of documents. This allows for non face-to-face documentary verification.

The AML/CFT Act also requires that reporting entities conduct verification of a customer's address using documents, data or information issued by a reliable and independent source.[1] This code of practice does not prescribe the way in which reporting entities can fulfil this obligation.

This code of practice does not apply to the identity verification of customers (that are natural persons) assessed by reporting entities to be high risk. Increased or more sophisticated measures should be applied for high risk customers.

[1] Sections 13, 16 and 24 of the Act

Legal obligations relating to identity verification
Subpart 1 of Part 2 of the AML/CFT Act outlines customer due diligence requirements. A reporting entity's AML/CFT programme, established under sections 56 – 57 of the Act, must include adequate and effective policies, procedures and controls for complying with customer due diligence requirements.

A reporting entity must base its AML/CFT programme, including its assessment of risk for the purpose of customer due diligence, on the AML/CFT risk assessment undertaken in accordance with section 58.

This code of practice applies to customers (that are natural persons) assessed by reporting entities as low to medium risk, for the verification of name and date of birth as required by:

i. Section 16 – standard customer due diligence: verification of identity requirements
ii. Section 20 – simplified customer due diligence: verification of identity requirements
iii. Section 24 – enhanced customer due diligence: verification of identity requirements[2]
iv. Section 28 – wire transfers: verification of identity requirements.

The Financial Markets Authority, Reserve Bank of New Zealand and the Department of Internal Affairs will consider reporting entities who comply with this code of practice to have met their obligations to verify name and date of birth under sections 16, 20, 24 and 28 of the AML/CFT Act for low to medium risk customers (that are natural persons).

Note: A word or expression used in this code of practice has the same meaning as in the AML/CFT Act (see section 34 of the Interpretation Act 1999).

What will you find in this code of practice?
This code of practice covers all reporting entities in all AML/CFT sectors.

This code of practice is in three parts

PART 1: DOCUMENTARY IDENTITY VERIFICATION

PART 2: DOCUMENT CERTIFICATION

PART 3: ELECTRONIC IDENTITY VERIFICATION

PART 1: DOCUMENTARY IDENTITY VERIFICATION

In order to conduct documentary verification of a customer's name and date of birth, the following is required:

[2] The Act requires enhanced due diligence in certain circumstances, however the Act does not predetermine that customers for whom enhanced due diligence is required be assessed as high risk. For example a politically exposed person might be assessed as a low to medium risk customer, but will always be subject to enhanced due diligence as required by section 24.

1. One form of the following primary photographic identification:

a) New Zealand passport
b) New Zealand certificate of identity issued under the Passports Act 1992
c) New Zealand certificate of identity issued under the Immigration New Zealand Operational Manual that is published under section 25 of the Immigration Act 2009
d) New Zealand refugee travel document issued under the Passports Act 1992
e) emergency travel document issued under the Passports Act 1992
f) New Zealand firearms licence
g) overseas passport or a similar document issued for the purpose of international travel which:

   i. contains the name, date of birth, a photograph and the signature of the person in whose name the document is issued; and
   ii. is issued by a foreign government, the United Nations or an agency of the United Nations.

h) a national identity card issued for the purpose of identification, that:

   i. contains the name, date of birth and a photograph of the person in whose name the document is issued and their signature or other biometric measure included where relevant ; and
   ii. is issued by a foreign government, the United Nations or an agency of the United Nations.

OR

2. One form of the following primary non-photographic identification:

a) New Zealand full birth certificate
b) certificate of New Zealand citizenship issued under the Citizenship Act 1977
c) a citizenship certificate issued by a foreign government
d) a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations

in combination with a secondary or supporting form of photographic identification, for example:

e) New Zealand driver licence
f) 18+ Card
g) valid and current international driving permit as defined in rule 88(1)(b) of the Land Transport (Driver Licensing) Rule 1999 and a licence from another country with a translation.

Points 2 (e) – (g) above are not an exhaustive list of secondary or supporting forms of photographic identification that may be acceptable. Reporting entities must ensure they are satisfied that any secondary or supporting photographic identification they accept is independent and reliable.

Confirmation that the identity information presented in the secondary or supporting form of photographic identification is consistent with the records held by a reliable and

independent source (for example the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995 or the Citizenship Act 1977 by the Department of Internal Affairs can be substituted for the primary non-photographic identification required in points 2(a)-(d).

OR

3. The New Zealand driver licence and, in addition, one of the following:

a) confirmation that the information presented on the driver licence is consistent with records held in the National Register of driver licences
b) confirmation that the identity information presented on the New Zealand driver licence is consistent with the records held by a reliable and independent source (for example the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Citizenship Act 1977, or the Passports Act 1992 by the Department of Internal Affairs)
c) a document issued by a registered bank that contains the person's name and signature, for example a credit card, debit card or eftpos card
d) a bank statement issued by a registered bank to the person in the 12 months immediately preceding the date of the application
e) a document issued by a government agency that contains the person's name and signature, for example a SuperGold Card as defined in the Social Security (SuperGold Card) Regulations 2007
f) a statement issued by a government agency to the person in the 12 months immediately preceding the date of the application, for example a statement from the Inland Revenue Department.

Note: Regulation 13(3) of the Health Entitlement Cards Regulations 1993 places strict restrictions on those who can legally demand or request a community services card as a form of identification. Reporting entities may accept a community services card under point 3(e) if the customer offers it; however they cannot request it.

4. In order to comply with this code, the reporting entity must have appropriate exception handling procedures in place, for circumstances when a customer demonstrates that they are unable to satisfy the requirements in 1 to 3 above.

5. Reporting entities must have a process in place to check that no other person with the same or similar names has presented the same identity information or documents.

6. Where documents are provided in a language that is not understood by the person carrying out the verification, an English translation must be provided.

7. In all instances where documentary verification is being used a reporting entity should verify the identity of the customer:

a) face to face; or by
b) copies of documents provided that are certified by a trusted referee (see below for certification requirements).

PART 2: DOCUMENT CERTIFICATION

8. In New Zealand a trusted referee must be at least 16 years of age and one of the following:

a) Commonwealth representative (as defined in the Oaths and Declarations Act 1957)
b) Member of the police
c) Justice of the peace
d) Registered medical doctor
e) Kaumātua (as verified through a reputable source)
f) Registered teacher
g) Minister of religion
h) Lawyer (as defined in the Lawyers and Conveyancers Act 2006)
i) Notary public
j) New Zealand Honorary consul
k) Member of Parliament
l) Chartered accountant (within the meaning of section 19 of the New Zealand Institute of Chartered Accountants Act 1996)
m) A person who has the legal authority to take statutory declarations or the equivalent in New Zealand

Certification when overseas

9. When certification occurs overseas, copies of international identification provided by a customer resident overseas must be certified by a person authorised by law in that country to take statutory declarations or equivalent in the customer's country.

10. In addition, the trusted referee must not be:

a) related to the customer; for example, a trusted referee cannot be their parent, child, brother, sister, aunt, uncle or cousin
b) the spouse or partner of the customer
c) a person who lives at the same address as the customer
d) a person involved in the transaction or business requiring the certification.

11. The trusted referee must sight the original documentary identification, and make a statement to the effect that the documents provided are a true copy and represent the identity of the named individual (link to the presenter).

12. Certification must include the name, signature, and the date of certification. The trusted referee must specify their capacity to act as a trusted referee from sections 8(a)-(m) above.

13. Certification must have been carried out in the three months preceding the presentation of the copied documents.

PART 3: ELECTRONIC IDENTITY VERIFICATION

14. An electronic identity is a record kept in electronic form that contains authenticated core identity information about an individual. Electronic identity

verification is using that record to verify an individual's identity when a reporting entity is conducting customer due diligence.

15. In order to conduct electronic identity verification of a customer's name and date of birth a reporting entity must;

a) verify the customer's name from either:
    a. a single independent electronic source that is able to verify an individual's identity to a high level of confidence; or
    b. at least two independent and reliable matching electronic sources.
b) verify the customer's date of birth from at least one reliable and independent electronic source.

16. Reporting entities must check the person's details against their customer records, to ensure that no other person has presented the same identity information or documents.

17. When determining what type of electronic sources will be considered reliable and independent, reporting entities must have regard to:

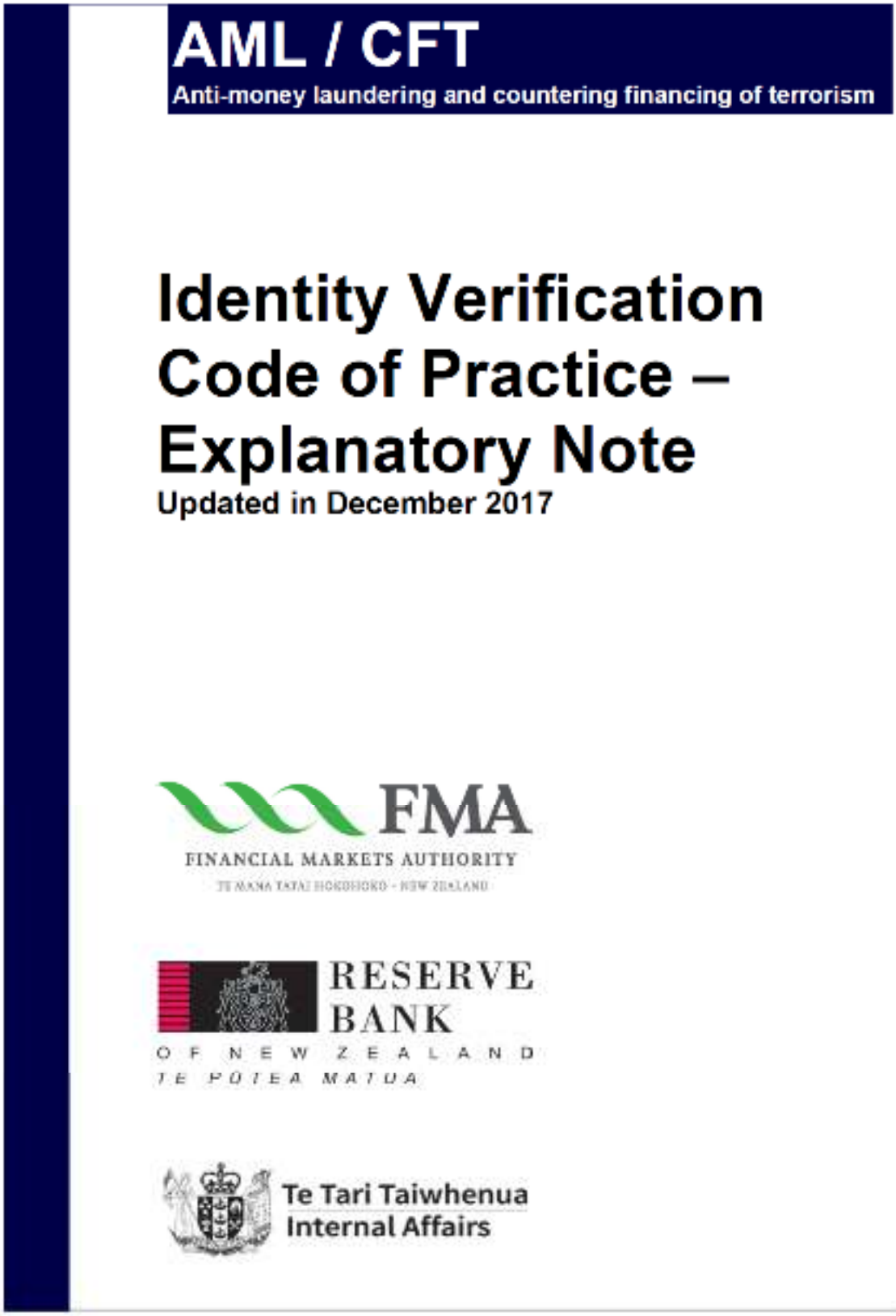
a) accuracy (how up-to-date is the information and what are the error rates and matching parameters);
b) security;
c) privacy (including whether the management and provision of the information is consistent with the Information Privacy Principles 5 to 11 in section 6 of the Privacy Act 1993);
d) method of information collection;
e) whether the electronic source has incorporated a mechanism to determine the customer can be linked to the claimed identity (whether biometrically or otherwise);
f) whether the information is maintained by a government body or pursuant to legislation; and
g) whether the information has been additionally verified from another reliable and independent source.

18. Reporting entities that use electronic identity verification methods must include information in their AML/CFT compliance programme that describes:

a) the forms of electronic identity verification methods that are considered reliable and independent and in what circumstances they will be used for the purposes of identity verification;
b) how the methods have regard to the matters described in clause 17; and
c) any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

Note: Nothing in this code of practice prevents a reporting entity from obtaining multi-source verification from a single provider, so long as they are satisfied that the requirements in Part 3 are complied with.

https://fma.govt.nz/assets/Reports/_versions/3222/131201-identity-verification-code-of-practice-2013-explanatory-note.2.pdf



Explanatory Note

1. This Explanatory Note should be read in conjunction with the Amended Identity Verification Code of Practice 2013. This note replaces the previous Explanatory Note that was published in October 2013.

2. The Amended Identity Verification Code of Practice 2013 (the code) clarified requirements for electronic identity verification following the implementation of the Electronic Identity Verification Act 2012 and the Identity Information Confirmation Act 2012. It replaced the previous Identity Verification Code of Practice 2011.

3. This Explanatory Note provides further clarification to reporting entities that seek to comply with Part 3 of the code by using electronic identity verification.

Electronic Verification

4. Electronic verification is considered to be where a customer's identity is verified remotely or non-face-to-face.

5. Electronic verification has two key components, firstly confirmation of identity information via an electronic source(s) and secondly matching the person you are dealing with to the identity that they are claiming (*i.e. are they the same person)?* Both components must be satisfied.

6. The electronic source is the underlying repository where the authenticated core identity information is held and against which an individual's identity is to be verified. In most circumstances, this is going to be information that is maintained by a government body or pursuant to legislation.

7. For electronic identity verification, it is important to remember that the electronic source is not any of the following:
   - The person that the reporting entity is dealing with online who provides their biographical information,
   - A selfie photo or video
   - An uploaded image of their identity document(s)
   - The email, application or internet platform that the reporting entity uses to receive this information or documents
   - The third party provider that a reporting entity uses to conduct its online electronic verification.

Using a single independent source

8. The code reflects that a reporting entity can satisfy electronic identity verification requirements from a single electronic source that is able to verify an individual's identity to a high level of confidence. Only an electronic source that incorporates biometric information or information which provides a level of confidence equal to biometric information enables an individual's identity to be verified to a high level of confidence.

9. Biometric information includes measurements of an individual's physical characteristics that can be recorded and used for comparison and automated recognition of that individual *e.g. photographs, iris structure or fingerprint information such as arch, whorl and loop types.*

Using two reliable and independent matching sources

10. The code also allows a reporting entity to verify an individual's identity from at least two electronic sources which must be:
    - Reliable, and
    - Independent, and
    - Match each other. [1]

11. Where two "reliable and independent" sources are used and they match each other, the "high level of confidence" required of a single independent source is not required.

12. Where two matching reliable and independent electronic sources are to be used, a reporting entity must still have regard to whether the electronic sources include a mechanism to determine if the customer can be linked to the claimed identity.

13. If the electronic sources do not contain this mechanism, additional or supplementary measures must be used to ensure the person that the reporting entity is dealing with is the genuine holder of the identity they are claiming to be.

Additional measures required

14. Clause 17(a) of the code requires a reporting entity to consider whether the electronic source(s) has incorporated a mechanism to determine whether the customer can be linked to their claimed identity (whether biometrically or otherwise). If the electronic source(s) does not have such a mechanism, or it is not robust enough, then a reporting entity is able to adopt additional measures that will be used to supplement it, or to otherwise mitigate any deficiencies in the process.

15. Some examples of additional measures include the following:

    - Require the first credit into the customer's account or facility to be received from an account/facility held at another New Zealand reporting entity in the customer's name.

    - Issue a letter that contains a unique reference/identifier to the customer's address that has been verified by a reliable and independent source. The letter/unique reference number must be returned to the reporting entity before the customer's account or facility is fully operational *e.g. before any withdrawals/debits can be conducted*.

[1] Note that it is possible for a reporting entity to verify an individual's identity from two or more 'reliable and independent' sources but via a single third party provider.

- Robust steps to confirm the authenticity of any identification document electronically provided by the customer. This should ensure that both the document belongs to the customer and that it has not been forged, altered or tampered with in any way *e.g. the original photo on the identification document is replaced.*

- Phone the customer on a number that has been verified by a reliable and independent source before the customer's account or facility is fully operational *e.g. before any withdrawals/debits can be conducted.*

- Robust security type questions based on reliable and independent information obtained about a person's social or financial footprint. This information should not be publicly available or easily obtained.

Inclusion with AML/CFT Programme

16. Reporting entities that utilise electronic verification must clearly describe in their AML/CFT Programme how all the relevant criteria within the code are satisfied. This includes any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

Customers who established a business relationship before 30 June 2013

17. Electronic sources could also be used to verify identity information for existing customers who established a business relationship with a reporting entity before 30 June 2013. Requirements in the code will still apply.

About codes of practice

18. Codes of practice are intended to provide a statement of practice to assist reporting entities to comply with certain Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) obligations. Codes of practice are dealt with in subpart 5 of the AML/CFT Act. Codes of practice set out the suggested best practice for meeting obligations. Some codes will cover all sectors, while others will be applicable to specific sectors or sub-sectors.

19. Complying with a code of practice is not mandatory. The AML/CFT regime allows for flexibility and scope for innovation because reporting entities can opt out of a code of practice. However, if fully complied with, codes of practice operate as a 'safe harbour'. The legal effect of a code of practice is described in section 67 of the AML/CFT Act.

20. If a reporting entity opts out of the code of practice it does not receive the benefit of the safe harbour. In these circumstances, the reporting entity must comply with the relevant statutory obligation by some other equally effective means. In order for this to be a defence to any act or omission by the reporting entity, the reporting entity must have provided written notification to its AML/CFT supervisor that it has opted out of compliance with the code and intends to satisfy its obligations by some other equally effective means.

Resources for the Amended Identification Verification Code of Practice 2013:

- Evidence of Identity Standard available on the Department of Internal Affairs' website
- Te Kāhui Māngai, a directory of Iwi and Māori organisations available on Te Puni Kokiri website.

5

Appendix 5 - Suspicious Activity

AML/CFT Act

39A Interpretation

suspicious activity means an activity undertaken in circumstances—

(a) in which—

(i) a person conducts or seeks to conduct a transaction through a reporting entity; or

(ii) a reporting entity provides or proposes to provide a service to a person; or

(iii) a person requests a reporting entity to provide a service or makes an inquiry to the reporting entity in relation to a service; and

(b) where the reporting entity has reasonable grounds to suspect that the transaction or proposed transaction, the service or proposed service, or the inquiry, as the case may be, is or may be relevant to—

(i) the investigation or prosecution of any person for a money laundering offence; or

(ii) the enforcement of the Misuse of Drugs Act 1975; or

(iii) the enforcement of the Terrorism Suppression Act 2002; or

(iv) the enforcement of the Proceeds of Crime Act 1991 or the Criminal Proceeds (Recovery) Act 2009; or

(v) the investigation or prosecution of an offence (within the meaning of section 243(1) of the Crimes Act 1961).

41Nature of suspicious activity report

(1) Except as provided in subsection (2), a report under section 40 must—

(a) be in the prescribed form (if any); and

(b) contain the details prescribed by regulations; and

(c) contain a statement of the grounds on which the reporting entity holds the suspicions referred to in paragraph (b) of the definition of suspicious activity in section 39A; and

(d) be signed by a person authorised by the reporting entity to sign suspicious activity reports (unless the report is forwarded by electronic means); and

(e) be forwarded, in writing, to the Commissioner—

(i) by way of secure electronic transmission by a means specified or provided by the Commissioner for that purpose; or

(ii) by another means (including, without limitation, by way of transmission by fax or email) that may be agreed from time to time between the Commissioner and the reporting entity concerned.

(2) If the urgency of the situation requires, a suspicious activity report may be made orally to any Police employee authorised for the purpose by the Commissioner, but in any such case the reporting entity must, as soon as practicable but no later than 3 working days after forming its suspicions, forward to the Commissioner a suspicious activity report that complies with the requirements in subsection (1).

(3) The Commissioner may confer the authority to receive a suspicious activity report under subsection (2) on—

(a) any specified Police employee; or
(b) Police employees of any specified rank or class; or
(c) any Police employee or Police employees for the time being holding any specified office or specified class of offices.