TOMPKINS | WAKE

Compliance Programme

Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Version 8 | July 31 2024

Contents

1.0 Introduction

Tompkins Wake is a 'Reporting Entity' under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. This Compliance Programme details the steps required for Tompkins Wake to fulfil its obligations under the act as a Designated Non-Financial Business or Profession (DNFBP). It is designed to ensure Tompkins Wake has policies, procedures, and training in place to detect, report and avoid all potential money laundering and terrorism financing activities. This programme is based on the firm's Risk Assessment. It should be read in conjunction with the Risk Assessment. This Compliance Programme, in conjunction with the firm's Risk Assessment, meets the firm's obligations under sections 56 and 57 of the Act.

The firm understands its obligations under the Act and has prepared this programme based on its knowledge of:

- The firm's Risk Assessment
- The AML/CFT Act
- National Risk Assessment
- Sector Risk Assessment
- Financial Intelligence Unit (FIU) Typology Reports
- Department of Internal Affairs guidelines and publications
- Financial Action Task Force (FATF) publications
- Advice from specialised AML/CFT advisers
- EIV provider processes.

The key areas to be improved from implementing and following this programme are:

- Formal identification of clients involved with activities captured under the Act
- Thorough assessment of the reasons and circumstances of any captured activities
- Formal identification of beneficial owners and persons with effective control
- Tompkins Wake Partners and staff being trained on how to identify potential money laundering and terrorism financing risk and how to assess clients at risk
- Tompkins Wake processes and procedures in line with industry best practices
- Effective use of AML/CFT software "Spinika" by all staff.

2.0 Risk Assessment

Tompkins Wake Board has an appetite for 'Low' risk.

This Compliance Programme has been prepared and implemented to meet this appetite. The firm operates in a 'Medium-High' risk sector.
The firm's inherent risk is assessed as 'Medium' based on the most recent Risk Assessment.

The residual risk after the implementation of this Compliance Programme will be low, provided all staff follow its processes and procedures.

Risk will be kept low through:

- ongoing Tompkins Wake Partner and staff training
- a risk assessment on all new matters
- existing client identification reviewed when there is a new matter and updated as required
- re-verifying clients if there is a material change or trigger to do so (see section 6.1 & 6.3)
- internal checks/reviews
- external audits

Tompkins Wake Board acknowledge that, based on the Risk Assessment, the likelihood of the firm being targeted or used for ML/FT is medium. The consequences if this did happen, however, are financially and reputationally severe.

Ensuring that Tompkins Wake staff never become either unwittingly involved or willfully blind to ML/FT risks is a priority for the firm.

Full details of the firm's ownership, senior managers, management structures, Tompkins Wake and activities can be found in the latest version of the Risk Assessment.

2.1 Managing and Mitigating ML/FT Risks

The firm's Compliance Officer and Compliance and Risk Lead will be primarily responsible for managing and mitigating Tompkins Wake's Money Laundering and Financing of Terrorism risks. These risks will be managed and mitigated through:

- Understanding and adhering to this Compliance Programme
- Effective utilisation of Spinika including the reporting and controls provided by this system.
- Staying up to date with relevant industry publications, any changes to the Act and guidance issued by the Department of Internal Affairs (DIA).
- Regular reporting to Team Leaders and Board
- All new client files opened must be reviewed and certified by a Partner for AML compliance (with only limited situations for delegation)
- Partners are ultimately accountable for AML compliance on all matters on which they are the supervising partner Ensuring a matter risk assessment is completed for every matter.
- Understanding and reviewing ML/FT red flags and being aware of new trends in ML/FT methods
- Training Tompkins Wake Partners and Staff on AML/CFT theory, awareness, the practice management system processes and this Compliance Programme.
- Training assist Partners and staff to detect trigger events and material changes within our client base that could indicate ML/FT risk
- Ensuring the current processes for managing the firm's trust account also include information gathering, CDD requirements and assessment of any ML/FT risks
- Establishing clear approval processes for delayed CDD, any exceptions and enhanced CDD
- Undertaking monitoring and internal spot audits to ensure the firm's policies and procedures are being effectively implemented.
- Regularly reviewing any high-risk clients.
- Undertaking vetting of any new Partners and staff that undertake captured activities.
- Ensuring both the Risk Assessment and Compliance Programme remain current and are reviewed at least yearly.
- Assessing and documenting the appropriateness of using any third-party service providers including electronic identity verification providers (EIVs) CDD agents, staff vetting agents and training providers (when applicable).
- Assessing any potential ML/FT risks if the firm launches any new product or service or makes an acquisition.

The above requirements have been documented within this Compliance Programme and the "Internal Controls Report" (or senior management reporting) can be used to record effective management and mitigation of the firm's ML/FT risks.

Reports are generated from Spinika to assist with managing AML/CFT risks.

This Compliance Programme has been formatted in a “Plain English” style to make it easy for staff to read and follow. Appendix I – “Technical References” summarises how the appropriate policies, procedures and controls have been documented throughout this Compliance Programme in alignment to the AML/CFT Act 2009.

3.0 AML/CFT Compliance Officer Selection

The AML/CFT Compliance Officer (referred to herein as the Compliance Officer) has been selected by the Board of Partners. For the purposes of the act the Board of Partners are considered the firms 'Senior Managers'.

Any changes to the Compliance Officer will need to be approved by the Board. The Board has decided that the role be held at the senior level of Partner and Philip Taylor has been appointed to this role.

The Compliance Officer selects the Reporting Officer. The role of Reporting Officer is held by Heather McLean

The Compliance Officer will be accountable for ensuring the firm meets its obligations under the AML/CFT Act. The Compliance Officer and senior managers are to be given additional training support and resources appropriate to ensure the firm's Risk Statement is adhered to.

If the Compliance Officer is unexpectantly absent, this role will be undertaken by Compliance and Risk Lead. For planned absences of more than four weeks, the Compliance Officer will appoint a replacement.

The Compliance Officer must report no less than twice yearly to the firm's Partners on matters relevant to this Compliance Programme, and the firm's obligations under the AML/CFT Act.

4.0 Undertaking AML

This section provides details on the activities undertaken by the firm that are captured by the AML/CFT Act.

AML must be undertaken for any captured activities.

4.1 Act Definition

Undertaking any of the following activities results in being captured by the Act:

a) Act as a formation agent of legal persons or legal arrangements
b) Arrange for a person to act as a nominee director, nominee shareholder or trustee in relation to legal persons or legal arrangements
c) Manage client funds (other than sums paid for professional services or other allowable low risk disbursements), accounts, securities, or other assets
d) Provide real estate agent work to effect a transaction
e) Provide a registered office or a business address, a correspondence address, or an administrative address for a company or partnership, or for any legal person or legal arrangement (unless that service is provided solely as an ancillary service to the provision of other services that are not captured)
f) Engage in or give instructions on behalf of a client to another person for:
    - Any conveyancing to effect a transaction (see section 5(1) for more detail)
    - A transaction within the meaning of section 4(1) of the Real Estate Agents Act 2008
    - A transfer of beneficial interest in land or other real property
    - A transaction on behalf of any person for buying or selling or transferring of a business or legal person and any other legal arrangement; or
    - A transaction on behalf of a client in relation to creating, operating, and managing

a legal person, and any other legal arrangement.

4.2 Captured Activities

The following activities are captured by the Act. A list of the captured activities undertaken by the firm is detailed in the Risk Assessment. See Attachment K for a full list.

Commercial	Conveyancing / Property	Trusts
Creation of a company	Buying or selling freehold property	Creation of trusts
Creation of a partnership	Transferring interests in property	Some Trustee Services (exclusions apply for family trusts)
Creation of a business-related trust or entity	Buying or selling leasehold interests	Managing client's investments
Creation of a charity	Giving instructions on behalf of clients	Giving instructions on behalf of clients
Buying or selling a business	Managing settlement proceeds	Registered office/address services*
Buying or selling business assets	Creation of leasehold interests	Authority to make payments from client's bank accounts
Changes in business shareholding or ownership that are tantamount to the buying or selling of a business	Creation of property ownership structures	Changes in trustees or beneficial ownership
Creation of financing arrangements	Leasing of commercial property	Trust administration
Registered office/address services*	Discharge of mortgage	

Estates	Family Law	Other
Buying or selling freehold property	Buying or selling freehold property	Client funds on deposit
Transferring interests in property	Transferring interests in property	Client funds held in trust account
Distribution of funds	Buying or selling leasehold interests	Wire (international) transfers >$1,000 (other than allowed low risk disbursements)
Managing client's investments	Giving instructions on behalf of clients	Litigation - distribution of settlement funds
Giving instructions on behalf of clients	Holding funds in trust	Managing client's investments
Executor of estates	Distribution of funds	Safe custody services
Beneficiaries over 25%		Cash transaction >$10,000
Estate administration		Authority to make payments from client's bank accounts

**Registered office and address services are only a captured activity if the service is provided in absence of any other material additional services.*

4.3 Use of Action Step Matter Types

The Matter and Sub Matter types will correctly classify whether the activity being undertaken for a client is captured or non-captured.

The full list of matter and sub matter types can be found in Appendix K.

4.4 Non-Captured Activity Declaration in Spinika

- Are you satisfied the new matter does not involve a captured activity?
- Have you considered whether this matter may lead to a captured activity?
- Are you satisfied there are no other aspects of the matter that trigger a requirement for CDD?

If you can answer 'yes' to all the above questions, CDD is not required, and you should complete the declaration in Spinika "I am satisfied that the work being undertaken in relation to this matter does not require the completion of CDD".

If you cannot answer 'yes' to all the above questions, CDD must be undertaken on your client.

4.5 Captured Advice

The firm's legal staff may give advice in relation to a captured activity (without necessarily carrying out the activity).

Generally, advice alone, in the absence of any actual captured activity, will not be caught by the definition. However, if over time it is anticipated that the staff member will be providing a mixture of advice and captured activities, client due diligence needs to be undertaken prior to establishing the business relationship.

Staff are to be aware of their obligations to report suspicious activities. This can include requests or enquiries about the services we offer from potential new clients (regardless of whether we ultimately provide those services).

4.6 Abnormal Transactions Activities and Enquiries

Abnormal transactions and activities that fall outside of Tompkins Wake's ordinary course of business or legal expertise need to be treated as high risk. If any such requests are made, the firm's Enhanced Client Due Diligence processes are to be followed.

Abnormal or unusual enquiries (that do not progress) should be escalated to the Compliance Officer to determine if there are grounds and adequate information to make a Suspicious Activity Report, as per section 12.1 herein.

4.7 New Services, Products or Delivery Channels

Before offering any new products, services, or delivery channels (such as entering a new area of practice, making acquisitions, or creating a new delivery/communication channel), a review of the AML/CFT Risk Assessment must be undertaken. Focus needs to be placed on any risks associated with any technologies that could increase a client's chances of staying anonymous. Additional policies, procedures and controls may need to be added to this Compliance Programme to mitigate any new risks highlighted in the updated Risk Assessment.

Prior to making any acquisitions the review should incorporate an evaluation of the target firms AML/CFT Risk Assessment and Compliance Programme along with a review of their most recent audit report and internal monitoring records. Focus should be on identifying potential new risks and areas of non-compliance that would need to be addressed as part of the acquisition process.

4.8 Occasional Transaction or Activity

A transaction or activity may occur in an occasional manner. Occasional does not necessarily mean "single"; it also includes circumstances in which multiple transactions are so intermittent or infrequent that no business relationship is established. When a person conducts an occasional activity or an occasional transaction through the firm, staff must comply with the requirements of the Act in relation to that person and undertake Client Due Diligence in accordance with the provisions of this Compliance Programme.

A situation in which an occasional transaction could occur is if the firm receives funds from a party to a transaction that is not a client of NZ$10,000 or more in cash. Cash means 'physical currency' and 'bearer-negotiable instruments' (which includes a cheque, bill of exchange, promissory note, bearer bond, traveller's cheque, money order, postal order or similar).
This also includes any wire transfers over NZ$1,000 (sending or receiving) that are undertaken for any non-client. This could occur if funds are refunded to a non-client or held for the benefit of a non-client.

‘Guidance: wire transfer requirement for designated non-financial business or professions’ indicates that an occasional transaction is most likely to occur when a contractual agreement is not met, and the non-client (or a person acting on their behalf) instructs the firm to refund or transfer the funds from our trust account.

Note that any instruction from a non-client to pay a third-party (rather than return/refund the funds to their point of origin) should be considered a red flag and may trigger Enhanced CDD as per sections 8 and 11 herein.

Where deposits that constitute” occasional transactions or activity” are paid into Tompkins Wake trust account ($10,000 or more), CDD will need to be undertaken on the purchaser even if we are acting for the vendor. We will require the Purchaser’s law firm or agent to provide us with current CDD documentation to satisfy our obligations.

5.0 Types of Client Due Diligence

This section provides information on the different levels of Client Due Diligence (CDD).

5.1 Client definition

A person or entity that the firm establishes a relationship with that results in the provision of a product or service.

An individual or a non-individual, e.g. a company, partnership, trust, Iwi or local authority.

A client is also someone who conducts an occasional transaction/activity (see section 4.6).

A client includes all associated parties, such as beneficial owners and persons acting on behalf of a client, identified through client due diligence and ongoing client due diligence processes.

Client Due Diligence is also commonly referred to as "Know Your Client". In this document, we will continue to refer to it as CDD to align with the AML/CFT Act definition.

CDD is the process by which a staff member develops an understanding of clients and the ML/FT risks they pose. CDD is completed for the client, any beneficial owners of the client, and any person acting on behalf of the client. There are three types of CDD:

- Standard
- Enhanced
- Simplified

5.2 Standard (CDD)

Standard CDD is the set of client due diligence enquiries/actions that staff must carry out for a client in situations where simplified CDD or enhanced CDD do not apply. Standard CDD is performed on the majority of clients, which are low and medium risk individuals, companies and limited partnerships.

(See sections 6 and 7 of this document for details of the information to be collected/verified for CDD clients.)

5.3 Enhanced (ECDD)

Enhanced CDD is a more substantial set of client due diligence enquiries/actions staff must carry out for clients considered a higher risk category for ML/FT. Enhanced CDD is performed on high-risk clients. Some examples are trusts, politically exposed persons, and entities with nominee director/shareholder/ partner relationships.

(See sections 6 and 8 of this document for a description of ECDD clients and details of the information to be collected/verified for them.)

5.4 Simplified (SCDD)

Simplified CDD is a simplified set of client due diligence enquiries/actions that staff must carry out for clients that qualify for simplified CDD. Performed on listed companies, local authorities, Crown entities, government bodies and registered banks.

(See sections 6 and 9 of this document for a description of SCDD clients and details of the information to be collected/verified for them.)

6.0 Client Identification and Verification

This section provides details on the activities undertaken by the firm that are captured by the AML/CFT Act.

6.1 Client Identification

Before undertaking any captured activity, all clients must be appropriately identified and verified (see the identification guidelines in Appendices A, B and C).

Identification and verification are mandatory for all staff when:

- commencing a new client relationship, or
- starting a new captured matter/activity for an existing client, when there is a material change or insufficient information.

Identification is the collecting of identity information from (or in respect of) the client.

Verification is the use of reliable and independent sources to verify or prove the identity information collected from (or in respect of) the client.

Verification is the process used internally by Tompkins Wake (if not using an electronic verification provider (EIV)). Any staff member can verify identification documentation provided by our clients if it meets the required standards detailed in this document.

Client Due Diligence (CDD) needs to be done as soon as practically possible (before establishing the relationship). Only on rare occasions should it be delayed.

New or existing clients undertaking a new matter with the firm are to be told they need to provide identification at their first meeting with staff and before engagement

Certification is a different process. Only qualified legal staff at Tompkins Wake can provide

certification to another entity and only certain people (trusted referees) can provide certified documentation to our firm. See "Appendix E – Acceptable Certifiers" for further information on certification processes and conditions.

Existing Clients Reengaging

Once a client has been identified and verified, there is no obligation to re-verify identity unless any of the following arise:

- there are doubts that the client exists or is who they claim to be
- a suspicion of ML or FT arises in relation to the client or an activity they undertake
- there is doubt as to the accuracy or adequacy of the information held on the client
- there is a material negative change to the risk profile of the client
- Ongoing Client Due Diligence (OCDD) indicates a need to re-verify the client (as per section 10)

When an existing client re-engages the firm to undertake a new matter activity, there is no obligation to re-verify identity unless any of the following arise:

- the client cannot be adequately linked to the identification already held on file
- the identification documentation on file is no longer accurate (does not include expiry date of ID)
- a suspicion of ML or FT arises in relation to the client or an activity they undertake
- there is a material negative change to the risk profile of the client
- Ongoing Client Due Diligence (OCDD) indicates a need to re-verify the client (as per section 10).
- The timeframe is 10 working days to complete this.

6.2 Identifying Beneficial Ownership and Effective Control

Beneficial owners are the individuals (natural persons) who ultimately own or control a client or on whose behalf a matter or activity is being conducted. They may also be those persons who exercise ultimate effective control over a legal person or arrangement.

Staff must verify the identity of any beneficial owner who ultimately, directly or indirectly, owns or has control, through one or more shareholdings or ownership of more than 25% or more of the

shares, voting rights, or ultimate benefit of the entity.

Where there are multiple layers in the ownership structure, staff are not required to complete full identification and verification on all the intermediate companies or entities in the ownership chain. Staff are required to follow the chain of ownership to the individuals who are the ultimate beneficial owners of the client and then complete the appropriate level of CDD.

Effective control may be exercised:

- directly through shareholding/ownership or the position they hold.
- indirectly through intermediate holding companies or influence.
- by those with power to manage funds or activities without requiring specific permission to do so, and who are in position to override internal processes, systems and controls and decisions.
- by providing instructions to a nominee whom they control (or who is accustomed to taking instructions from them).

Examples of beneficial owners and those who have effective control include:

- an individual who owns more than 25% of a company (shareholder)
- trustees of a trust
- partners of a partnership
- limited partners of a limited partnership
- individuals with the ability to control the client and/or dismiss or appoint those in senior management positions (or appoint trustees)
- individuals holding more than 25% of the client's voting rights
- individuals (for example, the CEO) in senior management positions

If beneficial ownership and/or effective control is unable to be determined, the Enhanced Client Due Diligence and escalation processes must be followed. (See section 8 of this document.)

If no one individual is identified as owning more than 25%, focus must be on verifying the individuals with effective control. Any owners involved in the activity/transaction or relationship with the firm should be verified as they are likely to have a level of effective control.

Some entities may have a large number of board members, directors, committee members or trustees. Examples can be large companies, co-operatives, incorporated and unincorporated societies, and iwi organisations. In certain circumstances, using a risk-based approach, you may choose to verify any of those people who are exercising effective control for the captured activity

being undertaken. The rationale for choosing not to verify other members (i.e. directors, members or trustees) should be documented and ML/FT risks must be assessed as low.

6.3 Identifying an Owner's Agent

A client may authorise another person to conduct matters/activities or act on their behalf.

Staff must determine the capacity in which a person (agent) is authorised to act on behalf of the client (i.e. power of attorney). Staff must identify and verify the following in respect of any agents (unless simplified CDD applies):

- Full name
- Date of birth
- Address or registered office
- Company identification or registration number
- Relationship to the client
- Evidence of authority to act as the person's agent
- Source of wealth if enhanced CDD applies

Approved third party agents may also be used to obtain a client's identification, verify this and provide the firm with certification they have done so. The use of any such agents (including electronic identity verification agents) needs to be approved by the firm's Compliance Officer.

If a third-party provider or agent is approved by the firm's Compliance Officer, the following steps are required:

- A thorough assessment of the provider is to be undertaken to ensure the services provided are consistent with the procedures detailed herein and the Identity Verification Code of Practice (IVCOP)
- Adequate controls are to be introduced to ensure the services provided remain consistently within approved standards
- This compliance programme is to be updated to reflect the services being provided and when they can be used
- The risk assessment is to be reviewed to consider any potential increased ML/FT risks associated with the new services

The Compliance Officer has approved the use of 'Real AML' assist with Client Due Diligence on behalf of the agency. The above four steps have been reviewed and 'Real AML' and are

considered an appropriate supplier of such services.

6.4 Verification Timing

Verification of a client's identity, address and source of wealth/funds must take place before work has commenced.

In rare circumstances verification of identity may be completed after the establishment of a client relationship only if all these circumstances are met:

- It is essential not to interrupt normal business practice
- Not progressing the matter/activity could breach our 'client care' obligations to act competently and timely to protect the client's interests.
- Any delay is in relation to the verification of identity only (i.e. identification documentation is still obtained pending the verification of this documentation)
- Any ML/FT risks have been identified; assessed as low and are being effectively managed
- Verification is being completed as soon as practicable after the initial contact with the client
- Approval is obtained (as per Section 8.3 of this document)
- Delayed CDD approval and monitoring is managed through the use of Spinika and the reports generated.

Day 0	Client onboarded – Client and Matter opened within Spinika
Day 7	Reminder 1 sent to Author and Legal Assistant
Day 14	Reminder 2 sent to Author and Legal Assistant noting Day 21 the Compliance Officer is notified
Day 21	Compliance Officer is notified, and a 'Delayed CDD Approval Form' is to be completed by the Author and approved by the Compliance Officer. Accounts team continues to report to Compliance Officer weekly until resolved.

Day 28	Supervising Partner is advised and actions to be file noted in Spinika including the possible need to withdraw from the matter and make a SAR

If it becomes apparent that the staff member may be unable to conduct or complete client due diligence on a client within a reasonable timeframe, they must not establish (or continue) a business relationship with the client. The staff member must consider making a Suspicious Activity Report and seek guidance from the Compliance Officer.

Unacceptable delays (or regular use of delays) are to be monitored by the Compliance Officer by maintaining and reviewing Spinika on a regular basis. Any concerns are to be recorded in the "Internal Controls Report".

6.5 Verification Methods

All proof of identity documents must be verified by a staff member, approved agent, or certified by a Trusted Referee. (See Appendices A, B and C).

Manual verification undertaken by staff (when EIV is not being used), is performed by:

- sighting the original document
- sighting the individual (when verifying ID)
- signing and dating a copy they have taken of the original and confirming "I verify this to be a true copy of the original, which I have sighted, and where it is an identity document the photo represents a true likeness of the individual named" (which confirms they have verified the original documents and sighted the individual)
- uploading the verified copy into Spinika (as per section 15.5).

Other verification options include:

- using Real AML' to undertake verification as an approved agent
- using 'Real AML' for a successful electronic identity verification (EIV)

Where possible, all ID documents need to be current. In some circumstances, ID documents can be expired up to a maximum of 24 months as per section 6.8 herein. Name and address verification must always be dated within the last 12 months.

The firm's practice management systems need to be checked to ensure no two clients with the same name have presented the same documentation for identification verification purposes. This

process is often done in conjunction with the firm's conflict checking procedures.

6.6 Electronic Identity Verification

The firm has decided staff can use Real AML' as a third-party electronic identity verification (EIV) provider in the normal course of its business. Staff must follow the provider's guidelines when undertaking electronic verification.

The Compliance Officer has the authority to choose and approve appropriate providers.

6.7 Reliance on other Reporting Entities

The firm can rely on identity and address document verification undertaken by another reporting entity. To satisfy this requirement, the other reporting entity should be considered reputable and reliable, and they should confirm that:

- They are a reporting entity under the AML/CFT Act and have a Compliance Programme in place to meet their requirements, and
- The CDD information they are sharing (or provided a reliance letter about) has been completed to the standard required by their AML/CFT Compliance Programme, and
- They have a business relationship with the mutual client, and
- They are not aware of any deficiencies in the CDD information the client provided, and
- They have record-keeping measures to at least the standard required by the Act, and
- They can/will provide us with the requested CDD information/documentation within five working days of any such request.

The firm remains responsible for ensuring CDD has been completed to the required standard as per Section 33 of the AML/CFT Act. Refer to the "Reliance on Shared CDD" guideline and "Shared CDD Consent" form for further information. Reliance letters need to be used in accordance with these guidelines.

6.8 Verification Exception Handling

Some clients (for example, the very young or elderly) may not be able to supply the ID documentation required under the AML/CFT Act.

The firm's exception handling process can be used in these circumstances, when:

- the reasons provided for being unable to supply ID are reasonable and all possible methods detailed herein have been exhausted
- ML/FT risks and red flags have been considered and there is no presence of heightened risk
- the client is a NZ resident or is a resident of a low-risk country.

The exception has been recorded, approved, and managed within the firm's AML Management System – Spinika.

Subject to the above, the following can be used for verification purposes:

- A statement from an authorised individual (who has known the client for more than 12 months) confirming their identity. CDD must be completed on the authorised individual and they must be of good character and be considered reliable.
- The Compliance Officer may approve use of the following expired ID documents (less than 24 months expired);
    - NZ passport
    - NZ certificate of identity
    - NZ firearms licence
    - NZ driver's licence
    - Emergency travel document
    - NZ refugee travel document
    - Overseas passport
    - National identity card
    - NZ Kiwi Access (18+) card (Hospitality Association).
- A document the Compliance Officer has approved a suitable alternative means of identification.
- One form of non-photographic ID should be provided as proof of residential address.
- The Compliance Officer may approve any suitable alternative means of identification when the above steps are not practicably possible.

6.9 Nature and Purpose

Understanding of both our client's 'nature' and 'purpose' must be recorded. The 'nature' of a client is understood by considering the following.

- Who are they and what is the rationale to any complex ownership structures?
- How did they come about their wealth or income (i.e. occupations)?
- If a business, what activities does the business undertake?
- Why are they engaging our services and how often are they expecting to engage us?
- What products or services do they want to use?
- Are they using other services in conjunction with our services?
- Are there advisors or intermediaries involved and if so, what are their roles?

The relevant information is to be recorded using Spinika (Nature of Relationship). Enhanced CDD may require a more in-depth description and Spinika is to be used for this purpose.

- The 'purpose' of a client is understood by considering the following.
- Why do they want the product or service?
- What will the product and service enable them to achieve?
- Is there a wider purpose to what you are doing for them?

A client's purpose will naturally be recorded within the matters contained within Action Step and Spinika as part of our onboarding and matter management processes. If required, additional records can be made using notes within Spinika.

7.0 Standard Client Due Diligence - CDD

Based on the firm's Risk Assessment, Standard CDD is likely to be the most common Due Diligence process used by staff. The requirements of each client type are detailed in this section.

Staff engaging with clients either now or in the foreseeable future undertaking a captured activity must complete Standard CDD (unless they meet the Simplified CDD criteria or qualify for Enhanced CDD).

Standard due diligence consists of both identification/verification and understanding the nature and purpose of the engagement to make an informed decision on potential ML/TF risk.

7.1 Individuals

Staff must collect, at a minimum, the following CDD information from an individual client:

- full name
- date of Birth
- physical residential address (where they reside)
- beneficial ownership or effective control relationships (if applicable)

If the client is a sole trader business, staff must also collect:

- the full legal or trading name
- the physical business address
- any beneficial owners or persons with effective control

To verify a client's name and date of birth, refer to Appendix A for acceptable forms of identification or use an EIV process (Real AML).

To verify a client's residential address, refer to Appendix B for acceptable documents, or use an EIV process (Real AML).

Information on the nature and purpose of the proposed business relationship between the client and the firm must be obtained, including the client's occupation. If the staff member determines an individual client poses a higher ML or FT risk (as per red flags detailed under section 11 of this document), the staff member must decide whether enhanced client due diligence should be applied.

7.2 Offshore Individuals

Due to the increased risk of ML/FT from individuals outside New Zealand, it is necessary to obtain a thorough understanding of their rationale for wanting to do business in New Zealand.

All reasonable attempts need to be made to verify these types of clients face-to-face (where possible). Trusted referees should be a last, or interim measure.

7.3 Partnerships

Some partnerships which are well known, reputable organisations (such as large legal and accounting firms) present lower ML/FT risk.

Smaller or less transparent partnerships can present heightened levels of risk. It is necessary to understand partnership structure and identify all relevant partners.

Staff must collect, at a minimum, the following CDD information:

- Full name
- Any trading names
- Business address, principal location/country of business and registered address (if applicable), and Identifier or Registration number (if applicable)
- Partner(s) – CDD as per Individuals as detailed herein if fewer than eight partners. If a partner is not an individual you must identify and verify the directors, or equivalent, of that entity. If the partner is not an individual and has an ownership interest of more than 25%, you must identify and verify the beneficial owners of that entity
- Information on the nature and purpose of the proposed business relationship with the firm, including the client's industry, products/services, and nature of their business

- Partnership deed where partnership shareholding is not evenly split or if a formal partnership deed is in place.
- Check for anyone with indirect control or the presence of any nominees (if not self-evident)

If the partnership has four or more partners all partners must be identified by name, date of birth and residential address. A minimum of four partners must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control.

These partners will include the individuals giving instructions to or holding the relationship with the firm.

If the partnership is registered in a foreign country and is looking to do business in New Zealand, it is necessary to understand why it wants to operate outside its home jurisdiction and maintain a business relationship with the firm. You should consider undertaking enhanced CDD as a precaution.

7.4 Private Companies - NZ Registered

Private companies can present heightened ML/FT risk as their ownership and management structures are less transparent than publicly listed or regulated companies.

It is necessary to thoroughly understand the legal structure, ownership, control, and the key individuals involved, including directors, shareholders and those who may have effective control.

Staff must collect, at a minimum, the following CDD information:

- Company name
- Company registered office (address)
- Principal location/country of businesses activities
- Company incorporation number
- Company office extracts
- If the powers that bind and regulate the company are unclear or complex, then a copy of the constitution may need to be obtained and verified to help determine beneficial ownership and control (i.e. to consider voting rights and how these can be enforced). This can normally be obtained from the New Zealand Companies Office register (documents tab).
- Directors – complete CDD as an Individual (as per section 7.1 of this document)

- Shareholders - identify and verify all beneficial owners holding more than 25%, and those with effective control; complete CDD as an Individual (as per section 7.1 of this document)
- If the shareholder(s) is a non-individual, you must identify the shareholders/beneficial owners of that entity and continue until a natural person is reached or any holding will be less than 25%.
- Information on the nature and purpose of the proposed business relationship with the firm, including the client's industry, products/services, and nature of their business.
- Obtain reasonable evidence on the existence of any nominee directors or shareholders. If this evidence is considered reliable and independent, it does not need to be verified (Enhanced CDD applies if nominees are present). The focus for identifying whether or not a director is a nominee for AML purposes depends on whether or not a director is acting independently.

A director is not a nominee for AML purposes where:

- they are a director of a TW Trustee Company (they are taking instructions from others); and
- the company structure is simple, and it is clear the directors and shareholders are not acting as nominees

A director is a nominee where:

- You, or a client, are acting as a director in place of a person who you are taking instructions from, or who is really directing the company

Further investigation is required where:

- Shareholders can be either. When you ask if there are any nominees you need to discover if they are acting independently or not. If they are acting independently, then they are not considered nominee directors, if they are, then the converse applies.
- When the company structure is complex, and it is not clear if nominees are present. Assurances may need to be sought to confirm the presence of any potential nominees.

If the company has four or more directors all directors must be identified by name, date of birth and residential address. A minimum of four directors must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control. These directors will include the individuals' giving instructions to or holding the relationship with the firm. The rationale for choosing not to verify all directors should be documented and ML/FT risks must be assessed as low.

If the company is registered in New Zealand but its principal location and/or activities are outside New Zealand, it is necessary to fully understand its reason for being registered in New Zealand while operating in another jurisdiction.

If the company is in liquidation, it is likely the liquidator is also a reporting entity and sharing CDD will be possible. A CDD process will be required on the liquidator, as they will have control and be acting on behalf of the company in liquidation. Refer to the DIA guidance for liquidators: www.dia.govt.nz/diawebsite.nsf/Files/AML-CFT-2024/$file/New-AMLCFT-regulations-for-liquidators.pdf

7.5 Private and Public Companies – Registered Offshore

As with NZ private companies, offshore private companies can present heightened ML/FT risk.

It is necessary to thoroughly understand the legal structure, ownership, control, and the key individuals involved, including directors, shareholders, beneficial owners, and those who may have effective control.

Staff must collect, at a minimum, the following CDD information:

- Company name
- Registered office address of the business
- Principal location/country of businesses activities
- Registration number
- Company office extracts
- If the powers that bind and regulate the company are unclear or complex, then a copy of the constitution may need to be obtained and verified to help determine beneficial ownership and control (i.e. to consider voting rights and how these can be enforced). This step is likely to be required for companies registered offshore.
- Directors – complete CDD as an Individual (as per section 7.1 of this document)
- Shareholders - identify and verify all beneficial owners holding more than 25%, and those with effective control; complete CDD as an Individual (as per section 7.1 of this document). If the shareholder(s) is a non-individual, you must identify the shareholders/beneficial owners of that entity and continue until a natural person is reached or holding is <25%; and
- Information on the nature and purpose of the proposed business relationship with the firm, including the client's industry, products/services, and nature of their business.

- Obtain reasonable evidence on the existence of any nominee directors or shareholders. If this evidence is considered reliable and independent, it does not need to be verified. This is a risk-based process so consider country risk and red flags as verification of this evidence may be prudent (Enhanced CDD applies if nominees are present). See section
- 7.4 for guidance on nominee roles.

When the company is registered in a foreign country and is looking to do business in New Zealand, it is necessary to understand why they want to operate outside their home jurisdiction and maintain a business relationship with the firm.

You must also obtain information on the source of wealth or funds of the client. Consider undertaking enhanced CDD as a precaution.

If the company is a publicly listed company on a recognised stock exchange (as per Appendix G), CDD does not need to be undertaken on the shareholders.

7.6 Incorporated or Unincorporated Entities

These types of entities include clubs, school boards, churches, societies, foundations and are usually small, local organisations serving a specific purpose (normally charitable).

Staff must collect, at a minimum, the following CDD information:

- Full name
- Legal status, incorporated or unincorporated
- Registration number, if incorporated
- Evidence of incorporation (if applicable)
- If the powers that bind and regulate the entity are unclear or complex, then a copy of the foundation document may need to be obtained and verified to help determine beneficial ownership and control.
- Address, registered address, if incorporated
- Directors/Officers/Governing Body/Trustees (controlling members) – identify and verify (all effective controllers or those with authority to act)
- Beneficial owners, if applicable - identify and verify all beneficial owners holding more than 25%
- Information on the nature and purpose of the proposed business relationship with the firm, including the entitie's activities, goals, and purpose (objectives and nature of their

operations).

If the entity has four or more controlling members all such members must be identified by name, date of birth and residential address. A minimum of four members must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control. These members will include the individuals giving instructions to or holding the relationship with the firm. The rationale for choosing not to verify all members should be documented and ML/FT risks must be assessed as low.

In the event such an entity/client is located in a foreign country, ECDD must be undertaken.

7.7 Limited Partnerships

Limited Partnerships can present as higher risk and ECDD should be considered as a precaution. Limited Partnerships may represent higher ML/FT risk given their potential complexity and unclear ownership.

Staff must collect, at a minimum, the following CDD information:

- Full name and any trading names
- Registered office address and principal country of business
- Registration number (if applicable)
- Limited partnership agreement showing the General Partner(s), Limited Partner(s) and a schedule if partnership shareholding is not evenly held. This will contain the details on the powers that bind and regulate the partnership.
- General partner(s) - identify and verify all. If the general partner(s) is a non-individual, you must identify and verify the directors, or equivalent, of that entity
- Limited partner(s) holding more than 25%. Identify and verify all beneficial owners holding more than 25%. If the limited partner(s) is a non-individual, you must identify the shareholders/beneficial owners of that entity and go back until natural persons are reached or holding is less than <25%
- If you choose to undertake ECDD, verify the source of funds or wealth of the client. This includes collecting the origin of the wealth (where relevant) and the source of any partnership income.
- Information on the nature and purpose of the proposed business relationship with the firm, including the partnership's industry, products/services and nature of the business.
- Obtain reasonable evidence on the existence of any nominee general partner. If this

evidence is considered reliable and independent, it does not need to be verified. (Enhanced CDD applies if nominees are present). See section 7.4 for guidance on nominee roles.

If the general partner is a company with four or more directors (or equivalent) all directors must be identified by name, date of birth and residential address. A minimum of four directors must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control. These directors will include the individuals giving instructions to or holding the relationship with the firm. The rationale for choosing not to verify all directors should be documented and ML/FT risks must be assessed as low.

When the partnership is registered/created in a foreign country and is looking to do business in New Zealand, it is necessary to understand why it wants to operate outside its home jurisdiction and maintain a business relationship with the firm.

7.8 Co-operatives

Staff must collect, at a minimum, the following CDD information:

- Full name
- Registration number (if applicable)
- Evidence of establishment and the powers that bind and regulate the co-operative
- Principal address and place of business
- Beneficial owners - identify and verify all beneficial owners holding more than 25%
- Individuals with effective control (senior managers) and/or the power to act on behalf of the co-operative (controlling members) - identify and verify all
- Information on the nature and purpose of the proposed business relationship with the firm

If the co-operative has four or more controlling members all such members must be identified by name, date of birth and residential address. A minimum of four members must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control. These members will include the individuals giving instructions to or holding the relationship with the firm. The rationale for choosing not to verify all members should be documented and ML/FT risks must be assessed as low.

7.9 Estates

If the Estate has an executor or administrator that is a 'Reporting Entity' staff must collect, at a minimum, the following information:

- Estate Name
- Evidence that the executor or administrator is a Reporting Entity
- Information on the nature and purpose of the proposed business relationship with the firm to identify any red flags/risks.

If Tompkins Wake is the executor or administrator of the estate, CDD does not have to be conducted in respect of the captured activities provided to the estate.

If Tompkins Wake is providing services to an executor/administrator that is also a reporting entity there is no requirement to conduct CDD on the executor or administrator.

In either situation, obligations to submit a Suspicious Activity report (SAR) if required and to have adequate record keeping, are still required.

If the executor or administrator is not a 'Reporting Entity' staff must collect, at a minimum, the following CDD information:

- Estate Name
- Address of the estate (may be one of the executors)
- Foundation documents such as probate/will/death certificate or letter of administration
- Executors - identify and verify all executors
- Discretionary beneficiaries - if the estates beneficiaries are considered discretionary, charitable, or it has more than 10 beneficiaries, provide a description of each class of beneficiary.
- Other Beneficiaries - name and date of birth of each beneficiary. Identify and verify those beneficiaries entitled to more than 25% of the estate's assets.
- Evidence of the source of funds or wealth of the estate. This does not need to be verified.
- Information on the nature and purpose of the proposed business relationship with the firm to help identify any red flags/risks
- Overseas payments may trigger a PTR.

8.0 Enhanced Client Due Diligence - ECDD

This section describes the processes and obligations when Enhanced Client Due Diligence (ECDD) is required.

ECDD must be conducted when clients present a higher risk or when a suspicious activity reporting obligation arises.

All staff must identify clients who present a higher ML/FT risk. (Section 11 of this document provides information on red flags and guidance to staff on when ECDD is required.)

8.1 Criteria for ECDD

ECDD must be undertaken when the client:

- has risks or red flags indicating a heightened level of ML/FT risk
- is a trust or a similar vehicle used for holding personal assets. This would include a company being used to hold personal assets (see 8.4)
- is an iwi organisation/trust (see 8.5)
- is a politically exposed person (see 8.6)
- is a non-resident and from a country with insufficient AML/CFT measures (see Appendix H)
- is a company or limited partnership with nominee directors, nominee shareholders or nominee general partners
- is involved with new and developing technologies that favour anonymity
- is a company with shares in bearer form
- is involved in (or undertaking) a complex or unusually large transaction
- is involved in (or undertaking) an unusual pattern of transactions that have no apparent economic or visible lawful purpose

Note that if a Trust is a shareholder of our "Client" ECDD is not automatically triggered as per bullet point two above.

8.2 Additional Information Requirements

ECDD involves collecting and verifying additional information for a more thorough assessment of the ML/FT risks of the client.

The following steps are required and must be done in conjunction with CDD or SCDD requirements.

- Collect and verify the client's source of wealth (SOW) and source of funds (SOF).
- Source of wealth are the activities that created the total net worth of the client. This will be required for all clients being subjected to ECDD.
- Source of funds includes the origin and means of transfer for any funds to be used in the client matter/transaction. This will be required if the captured activity being undertaken for the client involves (or enables) the movement of funds (in addition to SOW).
- Appendix D sets out examples of acceptable documentation for verification of the source of wealth and source of funds.
- Understand the purpose of the relationship with the firm and the matter/transaction, including a full understanding of the services sought and reasons for this.
- Understand the ongoing and expected activities of the client. This includes information such as the expected type of activity and transactions, whether domestic or international activity, countries dealt with, and other information deemed relevant to the expected nature of activity and services to be provided.
- If the client has been introduced by a third party, the staff member must understand the nature of introduction and the introducer. If the client will not be met face-to-face the reasons and rationale for this must also be understood.
- Complete the ECDD requirements and ensure a file note is made in Spinika in the 'Source of Wealth or Funds' section.
- As an alternative to obtaining source of wealth documentation, you can complete the "ECDD File Note" [Spinika] form if it is an existing client for five years plus with the firm, you have a good knowledge of their source of wealth and have evidence of their transactions that would support such knowledge. [to discuss this alternative]

8.3 Written Findings, Escalation and Approval Processes

The ECDD equivalent file notes and approvals are recorded within Spinika. Notes can be added to the following sections in Spinika:

- Source of Wealth or Funds - "Source of Wealth Details"
- Client Risk Assessment – "How do you evaluate the risk of ML/FT based on your knowledge of the matter and completed risk assessment"
- Client Risk Assessment – "Additional Client CDD Notes"
- CDD Unusual Activity – "Notes", "Activity being undertaken" "What is unusual about activity"

The firm's authorised approvers for ECDD are either a Partner or the Compliance Officer. [check this process and consider adding a lower level of basic family trusts] Approval should only be granted when the quality of the written findings and supporting verified documentation is of an acceptable standard.

The ECDD process is an important step in ensuring that the findings are kept in accordance with the requirements of the act. The findings are required even if an ECDD process does not progress to a Suspicious Activity Report.

If ECDD has been triggered due to country risk, the Compliance Officer should be notified for further instruction. This would include the additional measures taken to assess such risk, any restrictions imposed, and ongoing monitoring implemented for any such clients (as per section 10).

If ECDD cannot be completed due to insufficient information, the ECDD process needs to be completed and submitted to an authorised approver. The authorised approver is to determine if a suspicious activity report is required (as per section 12) and if the engagement should be terminated. If the business relationship is not terminated, then ongoing client reviews as per Section 10.5 of this Compliance Programme will be implemented

The following processes must be approved by the firm's authorised approvers: [review approval levels]

- Delayed CDD Approval
- Verification Exception Approval,

8.4 Trusts

The AML/CFT Act regards trusts as higher risk. All trusts must undergo ECDD. This includes trusts from large, nationally, and internationally active organisations to simple trusts for holding personal and family assets. Trusts represent higher ML/FT risk given their potential complexity and levels of anonymity.

It is important the ownership and control structure of the trust is clearly understood and the identity of key principals, such as trustees, is verified.

Staff must obtain the following information:

- Trust name
- Type of trust
- Address and Jurisdiction/Country of establishment
- Registration number, if applicable
- Original Trust Deed and subsequent amendments
- The presence of any settlor and/or protector of the trust needs to be established and verified (if not clearly established and verified using the Trust Deed)
- Trustee(s) - identify and verify all, where the trustee is a non-individual you must identify and verify the directors, or equivalent, of that entity
- Discretionary beneficiaries - if the trust is discretionary, charitable, or has more than 10 beneficiaries, provide a description of each class of beneficiary.
- Other Beneficiaries - name and date of birth of each beneficiary. Identify and verify those beneficiaries entitled to more than 25% of the trust's assets.
- Any individual with effective control over the trust or specific trust property and who benefits from the trust, or with the power to amend the trust's deeds or remove or appoint trustees. Identify and verify all including settlors, protectors, and appointers that have such powers.
- Any individual that can act on behalf of the trust. Identify and verify all.
- Verify the source of funds or wealth of the client. This includes collecting the name of the Settlor and the origin of the Settlor's wealth (where relevant) and the source of any income that the trust is receiving.
- Information on the nature and purpose of the proposed business relationship with the firm, including the trust's activities, goals, and purpose.

Staff must identify and verify the representatives who have authority on behalf of the trust, if the trustee is one of the following statutory trustee companies:

- Trustees Executors Limited
- Guardian Trust
- Perpetual
- Public Trust
- Māori Trust.

If the trustee is a non-statutory trustee company, such as a professional trustee company, staff must identify all the directors of the company and verify the identity of those who have authority on behalf of the trust. If this trustee company is also part of a reporting entity, using a risk-based approach the firm may choose to only verify the identity of those acting on behalf of the trustee company.

If the client is a discretionary trust (one where the trustees have discretion over the disbursement of trust assets), a charitable trust or one with more than 10 beneficiaries, staff do not need to obtain the name and date of birth of each beneficiary. However, they must obtain a description of:

- each class or type of beneficiary
- the reason and purpose of the trust (if the trust is a charitable trust).

If the trust is registered in a foreign country and is looking to do business in New Zealand, it is necessary to understand the reason for wanting to operate outside their home jurisdiction and to maintain a business relationship with the firm (in addition to the above information).

Verification of the identity and address of a trust can be obtained using one of the sources detailed in Appendix C.

8.5 Iwi Organisations/Trusts

Iwi can have several entity structures to hold assets. These entities have oversight through the Māori Land Court or having been established under legislation. They include:

- Post-Treaty Settlement Government Entities
- Mandated Iwi Organisations
- Recognised Iwi Organisations
- Iwi Aquaculture Organisations

- Māori Land Trusts (established under the Te Ture Whenua Māori Act 1993)

Staff must collect the following information for Iwi Organisations established under legislation:

- Name of organisation
- Registration number, if applicable
- Trustees/Directors or equivalent (controlling members). Identify and verify all, where the trustee is a non-individual you must identify and verify the directors, or equivalent, of that entity
- Beneficial owners (if applicable). Identify and verify those holding more than 25%.
- Verify the source of funds or wealth of the client. This includes collecting the origin of the wealth (where relevant) and the source of any income.
- Information on the nature and purpose of the proposed business relationship with the firm, including the organisation's activities, goals and purpose.

For Māori Trusts and Incorporations, staff must collect the following information:

- Trust or Entity name
- Type of trust
- Address
- Registration number (if applicable)
- Trustee(s) or Committee Management members (controlling members). Identify and verify all. Where a trustee or Committee management member is a non-individual you must identify and verify the directors, or equivalent, of that entity
- Beneficiaries - name and date of birth of each beneficiary or description of each class of beneficiary (see section 8.2 of this document for further information)
- Verify the source of funds or wealth of the client. This includes collecting the origin of the wealth (where relevant) and the source of any income.
- Information on the nature and purpose of the proposed business relationship with the firm, including the organisation's activities, goals and purpose.

Staff must always verify the entity and confirm its status as an iwi organisation or Māori Trust.

If the entity has four or more controlling members all such members must be identified by name, date of birth and residential address. A minimum of four members must have their identity verified, including all those who have an ownership interest of more than 25% and those with effective control. These members will include the individuals giving instructions to or holding the

relationship with the firm. The rationale for choosing not to verify all members should be documented and ML/FT risks must be assessed as low.

8.6 Politically Exposed Person (PEP)

Staff must consider and understand how to identify any PEPs, their close associates and close family members. This includes any that are beneficial owners of an entity.

Staff will become aware if a client is potentially a PEP while undertaking CDD. A formal EIV Provider PEP check will be performed on all new clients. This assessment can also be made by considering their personal information such as:

- past employment
- places of residence or employment
- where wealth/income was created
- if wealth/income has been provided by close associates or family members
- their operations and interests
- an EIV Provider report indicates a PEP status.

A PEP is a person who has held a prominent overseas position in the last 12 months. It includes close relatives and associates, and people with beneficial ownership of any legal entities or arrangements that benefit PEPs. Such positions would include:

- Head of State or head of a country or government; or
- government minister or equivalent senior politician; or
- Supreme Court Judge or equivalent senior Judge; or
- governor of a central bank or any other position that has comparable influence; or
- senior foreign representative, ambassador, or high commissioner; or
- high-ranking member of the armed forces; or
- board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any state enterprise.

If a staff member has grounds to suspect the client or any beneficial owner could be a PEP (based on the EIV check or information gathered from other sources), they need to:

- advise the Compliance Officer as soon as possible.

- complete ECDD and verify their source of wealth.
- consider undertaking additional formal PEP checks.
- obtain Compliance Officer approval to proceed (or not).
- determine the frequency of ongoing reviews of CDD (if retained as a client).
- perform Ongoing Client Due Diligence (OCDD).

The Compliance Officer is responsible for ensuring OCDD is undertaken by the staff member responsible for the PEP's relationship with the firm.

The Risk Assessment highlighted that the firm's exposure to PEP's is very unlikely. Tompkins Wake Partners and staff have been trained on how to identify PEP's by ensuring they understand the client. Our process is as follows:

- All clients should have a formal PEP check undertaken by a EIV provider.
- PEP checks should be updated if TW has reason to believe the client's situation may have changed resulting in an increased likelihood of them or a beneficial owner on the matter being a PEP.

Country risk is to be determined as detailed in Appendix H.

8.7 Technologies, Products, Services or Delivery Channels - Favour Anonymity

Clients involved with or using technologies, products, services, or delivery channels that favour anonymity present a higher level of risk and Enhanced CDD must be undertaken on any such clients. These types of clients can include (but are not limited to):

- Crypto/virtual currencies, assets, or exchange/wallet providers
- Unregulated services that enable exchange of value or money
- Communication services or channels designed to promote anonymity
- Unregulated lenders (pay day or cash), financial planners or mortgage brokers
- Unregulated online sales platforms or charge cards.

If the firm is considering using technologies, products, services, or delivery channels that favour anonymity, the firm's Risk Assessment must be updated. The assessment of any potential ML/FT risks must be undertaken prior to the introduction.

9.0 Simplified Client Due Diligence - SCDD

This section describes the circumstances, processes, and obligations for Simplified Client Due Diligence (SCDD).

SCDD does not exempt staff from having to obtain information on the nature and purpose of the proposed business relationship with the firm, or from performing Ongoing Client Due Diligence (OCDD). It does, however, have fewer requirements than standard and enhanced CDD.

SCDD can be applied to:

- entities listed on a recognised stock exchange (as per Appendix G)
- government departments and local authorities
- Crown entities
- regulated financial institutions
- licensed managing intermediaries or specified managing intermediaries
- entities supervised or regulated under the NZ AML/CFT Act and licensed or regulated in accordance with the Insurance (Prudential Supervision) Act 2010 and the Reserve Bank of New Zealand Act 1989.

If a licensed managing intermediary is a trust, ECDD is not required. Specified managing intermediaries also qualify for SCDD provided they confirm in writing the following:

- An AML/CFT programme in place and supervised for AML/CFT purposes
- Operating in accordance with the AML/CFT Act 2009
- Principal place of business in New Zealand.

If a client qualifies for SCDD staff must obtain the following information:

- Full name
- Address
- Evidence of status and SCDD qualification. This could include proof of listing, proof of regulation, evidence of Government status, evidence of licenses.
- Information on the nature and purpose of the proposed business relationship with the firm, including the client's industry, products/services, and nature of their business.
- If there are grounds to make a Suspicious Activity Report, then an Enhanced CDD process must also be completed.

When dealing with agents or certain approved staff of such clients, staff must obtain and verify the following information in relation to that agent or authorised person:

- Full name
- Date of Birth
- A person's relationship to the client and evidence of their authority to act.

If the firm undertakes a large volume of transactions for one client that qualifies for simplified CDD, one matter risk assessment can be undertaken for all of these transactions. If the matter varies in any way, a new matter risk assessment must be completed. For example, a standard easement for a utility provider.

In certain circumstances the agent (or approved staff member) may not need to be verified when acting by electronic means (such as email). These circumstances include when all of the following apply:

- a senior manager of the entity has provided identity information, and this has been verified; and
- the person acting on behalf of the entity is an employee; and
- the entity has entered into a written agreement with the firm setting out the required steps for employees to be delegated and authorised to act. This must include what electronic means are to be used and what the employee is authorised to carry out; and
- the senior manager has notified the firm the employee is authorised to act.

A senior manager is:

- a company Director; or
- a person who occupies a position comparable to that of a Director; or
- a person who holds a position that can exercise influence over the management or administration of the entity (i.e. a Chief Executive or a Chief Financial Officer).

9.1 Government Related Entities

This category includes certain local or overseas governments, Government departments and agencies and local authorities.

Where such a client is any of the categories in Appendix F, Simplified Client Due Diligence (SCDD) can be applied. If not, staff must obtain the following information:

- Full name
- Address
- Status
- Type of entity
- Authorised agents/staff. If the Government entity has eight or more authorised agents/staff, they all must be identified by gathering name, date of birth and residential address and a minimum of eight must have their identity verified. These must be the people principally responsible for giving instructions to the firm.
- Information on the nature and purpose of the proposed business relationship with the firm, including the client's industry, products/services, and nature of the business.
- If the client is based in a high or extreme risk jurisdiction, staff must obtain the names of all executive directors/senior management (i.e. CEO, CFO or equivalent). Staff must verify the identity of such executives if considered appropriate. Refer such cases to the Compliance Officer for guidance.

10.0 Ongoing Client Due Diligence

This section describes the circumstances, processes and obligations for Ongoing Client Due Diligence (OCDD).

Ongoing Client Due Diligence (OCDD) includes the processes that the firm adopts to ensure the client relationship and services remain consistent with our knowledge of that client.

OCDD ensures that once CDD has been completed the client's activities remain consistent with the CDD and their risk profile has not changed.

Given the nature of our client relationships being matter/event based often there is no ongoing activity to monitor. Ongoing monitoring is largely achieved by reviewing the CDD on file when an existing client approaches the firm to undertake a new matter and by ensuring our knowledge of the client has not changed between engagements. This includes the regular use of the Client/Matter Risk Assessments within Spinika and ensuring the information we hold about the client is current and still relevant.

OCDD can identify reasons for reporting a suspicious activity to the Financial Intelligence Unit (FIU), or it may give reason to revisit and update the CDD process/information.

10.1 OCDD Procedures

The firm has adopted the following OCDD procedures:

- Trust account transaction monitoring
- Trigger event reviews
- Material change reviews
- Multiple matter/activity reviews
- High risk client reviews every 12 months
- Extreme risk client reviews every six months

- Internal spot audits

Given the nature of the firm's business and the limitations of its practice management system, OCDD procedures are largely manual checks.

10.2 Trust Account Transaction Monitoring

The firm's trust account is operated in accordance with approved processes that meet NZ Law Society requirements. All financial transactions undertaken by the firm (on behalf of their clients) pass through the trust account.

In addition to the current processes, the Trust Account Administrators are to review all transactions daily and report any potential ML/FT risk to the Compliance Officer. The Compliance Officer will be obliged to also seek further information on any transactions that appear unusual or could indicate potential ML/FT risk.

- Any internal trust account payment audits will include a check that the firm's AML/CFT procedures are being complied with.
- The Trust Account Administrator and Compliance Officer need to be aware of the following red flags that require ECDD to be completed:
- Any complex or unusually large transactions
- Unusual patterns of transactions
- Any transaction/s that have no apparent economic or visible lawful purpose
- Any transaction that could be related to ML/FT

Other red flags to be aware of include clients where funds are being sent offshore or are high in velocity or frequency and any refunds or transfers requested by a non-client (occasional transaction) being directed to an account different from the origin of such funds.

10.3 Trigger Event and Material Change Reviews

If a staff member becomes aware of new or changed risks (an adverse material change) after the initial CDD then this will be a "trigger event" and a CDD review is required.

This also applies to existing clients that may not have had CDD completed. If any material change occurs, CDD should be undertaken at the first opportunity.

A staff member is to check for material change each time an existing client engages in a new captured activity by ensuring they understand the nature and purpose of the client and the service being provided, checking the information and documentation held on the client and then update Spinika with a new "Client/Matter Risk Assessment" to ensure this knowledge is consistent.

An example of material change includes (but is not limited to):

- Changes in ownership, control or beneficial owners (i.e. directors, trustees, shareholders, beneficiaries).
- Changes to the nature and purpose of the client.
- Changes to the client's risk profile
- Changes to foundation documents.
- Staff become aware of changes to/or new evidence of source of wealth and/or funds.
- Changes in client behaviour (i.e. an inactive client becomes active)
- Previous documentation relied upon for CDD purposes is no longer considered reliable or accurate.

The extent of the review (either CDD or ECDD) will be dependent on the extent of the increased risk identified. It will require CDD or ECDD to be newly completed.

In certain circumstances, a Suspicious Activity Report may need to be considered (see section 12.1 of this document).

10.4 Multiple Matter/Activity Reviews

Clients undertaking a high number of multiple matters or activities with the firm could present a higher level of potential ML/FT risk.

If a client materially increases the amount of activity after the initial CDD or refers associates that then undertake a high level of activity, a CDD review is required.

The extent of the review (either CDD or ECDD) will be dependent on the extent of the increased risk identified. It will require CDD or ECDD to be newly completed.

10.5 High and Extreme Risk Client Reviews

If a client (or beneficial owner) is assessed as high risk or extreme risk, ECDD will have been undertaken and any ML/FT risk deemed acceptable. This type of client includes:

- All PEPs
- Clients operating in high or extreme risk jurisdictions
- Clients associated with or who provide products and services that are considered new or developing technology, that may favour anonymity
- Clients where the verification of SOW/SOF was not considered sufficient (or available), yet the relationship was not terminated.
- Any client in respect of which a SAR (Suspicious Activity Report) has been raised
- Any other client identified as being high or extreme risk

High risk clients will have ECDD revisited yearly, or at the next possible opportunity (i.e. before the firm undertakes any further activity with the client).

For clients for whom the verification of SOW/SOF was not considered sufficient (or available) at the time of the matter/captured activity, it is to be revisited at a time when SOW/SOF documentation is expected to be sufficient and available for verification or at the next possible opportunity (i.e. before the firm undertakes any further activity with the client).

10.6 Internal Spot Audits

The firm will undertake spot audits on clients to check that this Compliance Programme's AML/CFT procedures have been followed. Spot audits will be undertaken on clients that may present higher ML/FT risk and on a random selection of clients.

No less than sixty spot audits will be undertaken each six months. Spot checks can be undertaken by any staff member nominated by the Compliance Officer considered capable of undertaking the audit. A copy of the spot audit results is to be reported to the Compliance Officer and retained.

If a client has an ongoing active relationship with the firm, then these clients should be included/considered in the spot audit sample. When selecting clients for a spot audit, a check should also be undertaken on a selection of matters that have been coded as non-captured. Such a check is to ensure that all captured activities are being identified and that a non-captured matter code is not being used to record both non-captured and captured activities/matters.

11.0 Assessing Risk and Red Flags

When undertaking any CDD, staff must gain adequate knowledge of the client and the activity/matter to assess any potential ML/FT risk. This section details the red flags staff need to be aware of.

Staff are required to consider "Red Flags" when undertaking any CDD. The list of red flags below is not exhaustive and should be used in conjunction with general observations, experience and judgement of character and new client and/or matter risk assessment. Using a risk-based approach, the employee is to decide if enhanced client due diligence is required based on:

- the severity of the red flag(s)
- the number of red flags present
- their own conclusion to the possible presence of potential ML/FT risk
- discussion with colleagues and/or the Compliance Officer If ECDD is required, refer to section 8.0 of this document.

If staff become aware of "Red Flags" after completing CDD, a "Trigger Event and Material Change Review" must be considered (as per section 10.3). All staff are to use the Client Risk Assessment and Matter Risk Assessment within Spinika when undertaking any captured activity.

Matter Risk Assessment	Client Risk Assessment
▶ Is the structure of the matter overly complex or an unusually large transaction? If yes - enhanced	▶ Is the client eligible for Simplified CDD per 18.2 of the AML/CFT Act 2009? If yes, simplified
▶ Does the economic or commercial rationale for the matter NOT make sense? If yes - enhanced	▶ Is the client a trust, estate, iwi organisation or other vehicle for holding personal assets? If yes, enhanced

▶ Does the rationale for the firm's involvement in this matter NOT make sense? If yes - enhanced	▶ Is the client a company with nominee directors and/or shareholders, general partners or shares in bearer form? If yes, enhanced
▶ Is a related party on this matter a politically exposed person (PEP)? If yes - enhanced	▶ Is the client or related party a Politically Exposed Person (PEP)? If yes, enhanced
▶ Is the matter involved with new technologies / products favouring anonymity? If yes - enhanced	▶ Is the client involved with new technologies/products favouring anonymity? If yes, enhanced
▶ Does the matter involve dealing with a related party from or connected to a country that that is identified	▶ Is the client or related party connected to a country that is identified by a Financial Action
▶ by the Financial Action Task Force (FATF) as lacking AML/CFT systems? If yes - enhanced	▶ Task Force (FATF) as lacking AML/CFT systems? If yes, enhanced
▶ Does the matter involve a country that poses a higher risk according to the Basel AML index? If yes - enhanced	▶ Is the client or related party from a country that poses a higher risk according to the Basel AML index? If yes, enhanced
▶ Will the firm handle client monies/proceeds for this matter?	▶ Does the client's behaviour give rise to any concerns (evasive, secretive, etc.)?
▶ Are there aspects of the matter we will not be involved in, where we normally would be?	▶ Does the rationale for the firm's involvement with this client NOT make sense?
▶ Does the matter involve more than $10m?	▶ Have you or your colleague NOT met the client face to face?
▶ Are there any aspects of the matter where you will not be dealing directly with the client?	▶ Is the client a non-resident?
How do you evaluate the risk of money laundering and terrorist financing based on your knowledge of the matter and completed risk assessment (low/medium/high)?	How do you evaluate the risk of money laundering and terrorist financing based on your knowledge of the client and completed risk assessment(low/medium/high)?
Please share the key factors and reasoning behind your risk score	Please share the key factors and reasoning behind your risk score

Any "yes" responses require comments to be made within Spinika. When required, Enhanced CDD should be undertaken as per section 8 herein. Unusual Activities can be submitted within GoAML.

Other red flags based on guidance material include:

General Red Flags
▶ Non-face-to-face contact without good reason
▶ Country risk medium or higher (clients, funds, wealth, or related parties) - see Appendix H
▶ Unreasonable speed required or engaged late in a transaction/matter
▶ Disproportionate amount of cash
▶ Funds from non-taxable transactions
▶ Multiple legal advisors or changes in legal advisors, or multiple intermediaries involved.
▶ Unrelated parties connected without a clear business reason
▶ Service required was refused/terminated by another professional
▶ Finance provided from a non-reputable or unknown source without reasonable explanation
▶ Client remotely located from firm with no clear reason to be using services remotely
▶ Client unconcerned about legal fees or offering payment in advance
▶ Authority to act on behalf of a client/individual without reasonable explanation or multiple intermediaries involved.
▶ Client is unusually curious about compliance procedures
▶ Client asking you to act outside of your area or expertise
▶ Legal documents too simplistic for the transaction
▶ Cash smelling of drugs, chemicals or musty

Red Flags Activities
▶ International wire transfers (telegraphic transfers)
▶ Use of products and transactions that favour anonymity (i.e. virtual assets, exchanges and offices)
▶ Structured transactions to avoid reporting thresholds
▶ Cancelled transactions after receipt of funds
▶ Late changes to settlement or execution instructions with no logical explanation
▶ Aborted or quickly resolved litigation involving payment of funds (sham litigation)

Payments to third parties contrary to contractual obligations
Use of firm's trust account to make payments to third parties with no logical explanation
Making unusual investments or purchasing unusual securities
Deposits for cancelled matters being refunded to different party
Unusually large transaction
Structure supports aggressive tax planning/evasion or involves low/no tax jurisdictions
Use of firm's trust account to make payments to third parties with no logical explanation
Making unusual investments or purchasing unusual securities
Deposits for cancelled matters being refunded to different party
Unusually large transaction
Structure supports aggressive tax planning/evasion or involves low/no tax jurisdictions

Red Flags for Property
Buying or selling unsighted with little interest in the property's features
Buying or selling a property with no reasonable explanation of the reason
Price paid or expected is unusually high or low (or indifferent to price)
Manipulation of the appraisal or valuation
Buyers and sellers colluding suspiciously
Funds received from multiple individuals or sources
Disproportionate amount of private funding
Unusual/complex source of funds
Buyer's or seller's agent particularly guarded about their client
Back-to-back transactions with increasing value or occurring in quick succession
Unusual volumes of transactions
Mortgages repeatably repaid rapidly with no clear reason

Red Flags for Businesses
▶ No New Zealand directors or token directors or it is unclear who has ultimate control
▶ Cash intensive businesses
▶ Excessive drawings or living beyond means
▶ Registered in a high-risk jurisdiction (see Appendix H)
▶ Unusual number of employees
▶ Business activities mainly outside of New Zealand
▶ Access to banking facilities a priority
▶ Use of false or overly simplistic documents
▶ Use of unusual email domains and/or difficult to find on the internet
▶ The businesses normal activities do not match the types of products of service being acquired
▶ Providing services for, or making investments in foreign companies that have unusual or high-risk activities
▶ Transfer of assets between businesses with common owners/control without a logical business reason
▶ Rapidly increasing or unusual changes in capital with no logical explanation
▶ Involved in the sale or purchase of luxury items internationally
▶ Lack of public information available on the business and its activities
▶ Possible blending of legitimate business income with illegitimate income

Red Flags for Trusts and Charities
▶ Not for profit organisations with unclear operations
▶ Use of intermediaries without good reason
▶ Attempts to disguise the real owner/s or parties
▶ Overly complex ownership or management structures
▶ Excessive or unusual use of nominees

▶ Unusual use of intermediaries or multiple intermediaries
▶ Purchase of large assets by a charity that are sold or transferred within a relatively short period of time
▶ Undertaking transactions not compatible with the stated purpose

Red Flags for Industries
▶ Less known or unreputable financial service providers
▶ Money service businesses or remitters
▶ Trade in commodities that can be dually used in missiles, and chemical, biological and nuclear weapons
▶ Trade in exotic or rare items and animals
▶ Embassies and consulates
▶ Casinos and gambling services

Extreme Risk (refer to Compliance Officer for guidance)
▶ Shell and correspondent banks
▶ Bearer shares
▶ Crypto currencies, virtual assets and exchanges
▶ Protected entities from jurisdictions that allow anonymity

12.0 Reporting - Suspicious Activity and Transactions

This section details the firm's escalation processes, the types of reporting required and how to submit reports.
.

12.1 Suspicious Activity Report - SAR

The firm must report to the Financial Intelligence Unit (FIU) where, during the course of our business, we suspect a person is engaging in money laundering, financing of terrorism or any other criminal activity.

The Reporting Officer must complete the suspicious activity report (SAR) where they suspect that a person is engaged in or attempting to engage in ML/FT or other criminal activity as soon as is practically possible. This SAR report along with the ECDD documentation needs to be given to either the firm's Reporting Officer and/or Compliance Officer before submission. Ensure the "ECDD process" is comprehensive as quality written findings are required to be retained even if the Compliance Officer decides not to submit a SAR.

The Reporting Officer and Compliance Officer will help determine whether the SAR report needs to be submitted to the FIU. If the officer determines a suspicious activity reporting obligation has been triggered, they must report the matter to the FIU within three business days from forming their suspicion (urgent SAR's can initially be made orally). A copy of the report and supporting documentation must be held by the firm.

If the Reporting Officer and Compliance Officer determines that a SAR does not need to be submitted to the FIU, they are to document any steps taken to conduct ECDD including obtaining and verifying source of wealth. They must record the reasons for making the decision not to submit a SAR using a file note.

All SARs will be saved in the practice management system under – AML Suspicious Activity Reports.

If ECDD results in a suspicious activity report (SAR) being required, the procedures detailed in sections 8.2 and 8.3 in this document must have been undertaken. Before the SAR is submitted, the Compliance Officer is to review and approve its submission.

If the submission of a SAR is being considered, and this is not the result of an ECDD, this must be escalated to the Compliance Officer. The Compliance Officer will determine what additional steps are required prior to submitting the report. Section 22(a) of the Act requires ECDD to be conducted as soon as practicable after becoming aware that a suspicious activity report is required.

12.2 Prescribed Transaction Report - PTR

A prescribed transaction report (PTR) is required to record all international wire transfers of NZD$1,000 or more and all physical cash transactions of NZD$10,000 or more. This includes any such transactions into or from our trust account. PTRs must be reported to the FIU within 10 business days of the transaction.

During the daily reconciliation of the trust account, it will become evident whether any international wire transfers have been made/received. When such payments are identified, these are escalated to the Reporting Officer for reporting to be completed within 10 business days. Entered via Go AML by the Trust Manager.
To avoid doubt, the firm will be required to submit a PTR if an international wire transfer is made from the firm's trust account. Passing on a client's instructions for a wire transfer to be made is not captured.

To avoid doubt, any international wire transfers directed to the firm's trust account when originated offshore will be captured.

While ANZ Bank may be required to also submit a PTR in relation to the same wire transfer of funds, the two PTR's will never be identical. Consequently, our PTR is not considered duplicate but complementary reporting.

It is likely that the information required in submitting a PTR will either have been provided by the client to make an outbound international wire transfer or ANZ Bank will provide this information through trust account reporting for any inbound wire transfers. If any payment is unidentifiable in terms of the international wire transfer provisions, contact needs to be made with ANZ Bank to obtain the prescribed information, this will assist in identifying potential international wire transfers.

The information that is required by the PTR regulations include:

- Specified details regarding the transaction.
- Specified information regarding our client. This will have been collected as part of the CDD process and must also include a unique identifier such as a matter number, client code, or reference number.
- Specified information regarding the beneficiary or originator of the international wire transfer.

If the firm has received cash of $10,000 or more from a client, a PTR must be completed. Cash transactions represent heightened ML/FT risk and the presence of these must be taken into consideration when completing CDD. They must be escalated to the Compliance Officer. The Compliance Officer is to review them before being submitted by the Reporting Officer.

All PTR's will be saved in the practice management system under – AML Prescribed Transaction Reports - 503467-16.

Prescribed transaction reports (PTR's) can be made by the Reporting Officer or finance staff processing the transaction. These only need to be escalated to the Compliance Officer if there have been ML/FT risks identified.

12.3 goAML – FIU Reporting Portal

SARs and PTRs must be submitted to the FIU using its online portal goAML. The firm's Reporting Officer and/or the Compliance Officer will be primarily responsible for maintaining the profile in goAML, preparing, and submitting reports to the required standard.

goAML website: https://fiu.police.govt.nz/Home

The Reporting Officer and/or Compliance Officer will have a copy of the Quick Reference Guide issued by the FIU. Staff must use the firm's AML/CFT forms and processes to ensure correct client information is held for completing SARs and PTRs.

The "Internal Controls Report" can be used to monitor the number and quality of any PTR's and SARs submitted. This should include checking that they have been filed within the required timeframes, include sufficient information, and are accepted by the FIU.

goAML does not store SARs or PTRs for longer than 10 days. A copy of any report submitted must be retained by the firm for five years. goAML can provide a hard copy and electronic

copies of the reports. These reports should not be held on the client's file as they are confidential between Tompkins Wake and the FIU.

12.4 Legal Privilege and Tipping Off

Staff must not disclose to clients that a suspicion has been formed or a report has been lodged with the FIU. This includes, where possible, not indicating to clients (through their actions) any suspicion. Care must be taken during all enquiries undertaken as part of the ECDD process that a client is not 'tipped off'.

Unauthorised disclosure by an employee constitutes an offence. It may subject the employee to criminal prosecution, as well as exposing the firm to severe penalties.

The presence of potential legal privilege should not stop CDD or ECDD being undertaken. Legal privilege, however, needs to be considered before submitting a SAR to the FIU. If a lawyer believes on 'reasonable grounds' the information obtained is legally privileged, then a SAR cannot be submitted, or the information contained within the SAR will need to be altered so not to disclose the privileged content.

This does not apply to confidential information which must be disclosed as required. The processes in Section 8.3 of this document will ensure legal privilege is considered at the appropriate approval level.

The NZ Law Society has issued guidelines on legal privilege (Preparing for AML/CFT – Privilege, confidentiality and reporting suspicious activities) that should be considered prior to any SAR not being submitted or altered on the grounds of legal privilege.

13.0 Employee Due Diligence

This section details the due diligence required on the firm's employees. A risk-based decision was made not to vet our existing employees prior to the Act coming into effect.

Given the presence of captured activities undertaken by the firm, every new employee (including temporary staff and contractors) must undergo, where possible, the following checks before starting at the firm:

- Police record check or Ministry of Justice criminal record check (where that employee is not already subject to a recent criminal check e.g. as part of being granted a practicing certificate).
- Legal right to work
- Proof of identity as per CDD herein
- Past employment confirmation
- Past employment referee, verbal check
- Credit check (optional)
- Sanctions/PEP check (if appropriate)

If the checks cannot be practicably completed before the employee commences the role, the role must be subject to such checks being completed and acceptable to the employer. The employer must retain the right to terminate the employment if a subsequent check is unacceptable.

Such checks must also be considered when someone within the firm is newly appointed to the role of either Compliance Officer, Reporting Officer, Trust Account Administrator, or any Senior Management appointment.

Additional checks on staff (including existing staff) must be carried out when certain trigger events occur:

- It appears an employee has failed to raise an SAR or PTR in circumstances where the firm would have expected the employee to have done so.
- An employee continually fails to adequately follow the processes in this Compliance

Programme.

- A suspicious activity report is made in relation to an employee.
- The employee is identified as presenting an elevated fraud or other security risk.

Employee due diligence must be undertaken by someone involved in the recruitment process within the firm and/or holding a position more senior than the employee, or the Compliance Officer.

The Compliance Officer is to approve the use of any third-party vetting agents. The use of vetting agents must be in line with the above requirements and assessed and managed using the 'Institutions' section of the firm's Risk Assessment and 'Employee Due Diligence' section of the Internal Controls Report.

14.0 Training Requirements

This section details staff training requirements under the AML/CFT Act.

The firm will ensure all staff, partners and senior management receive appropriate training in identifying suspicious activity and their obligations under this Compliance Programme.

Training will be ongoing to ensure employees are informed of new developments, including information on current ML and FT techniques, and methods to help them recognise what might constitute suspicious activity in relation to their area of practice.

14.1 Training Content

Staff and senior management training must be designed internally and/or sourced externally to:

- Raise awareness among staff as to the risks of ML/FT, the relevant legislation that applies to them and their obligations under that legislation.
- Raise awareness of the impacts of ML/FT on the firm and the potential effect on the firm and our staff from non-compliance with the AML/CFT Act. It is important that senior management understand the implications associated with potential non-compliance.
- Highlight specific ML/FT risks relevant to the practice areas of staff/firm.
- Ensure staff know how to complete CDD correctly and identify red flags/risks that would trigger an Enhanced CDD process or SAR.
- Ensure familiarity with the controls, processes, and requirements in place to address those risks.
- Ensure correct use of reporting procedures such as the use of AML Online (DIA) and goAML (FIU) portals (if applicable).
- Highlight and remedy any issues identified from internal/external audits and monitoring.
- Inform employees that appropriate disciplinary action, including dismissal, may follow from a breach of the AML/CTF Act and/or this Compliance Programme in appropriate circumstances

.

The relevance and appropriateness of the training programme must be regularly reviewed by the Compliance Officer. A training register is to be maintained to monitor all training activities and highlight any deficiencies.

14.2 Training – Staff Requirements

The firm has decided all staff are to undertake formal training annually. It is expected that such training is likely to include at least 45-60 minutes of AML/CFT CPD compliant content.

The Compliance Officer has the authority to waive this training requirement for staff that do not undertake captured activities as per the definition contained within the AML/CFT Act (as per section 4.1).

The Risk Assessment has not highlighted any staff requiring training more frequently than annually although staff may be given other AML training modules to help them with specific aspects of their roles.

The Compliance Officer Compliance and Risk Lead will undertake additional training relevant to assisting them with their obligations in this role. It is expected this will include, as a minimum, an additional 45-60 minutes of AML/CFT applicable content annually.

This additional training may include a combination of:

- Attending conferences or events related to AML/CFT
- Engaging with external AML/CFT consultants
- Reading related industry articles
- Attending webinars or viewing recorded AML/CFT video content
- Relevant training provided by the DIA or Police FIU including the correct use of the AML Online and goAML portals.
- Staying up to date and understanding any changes made to the core knowledge resources detailed in section 1.0 of this document

Records of all staff AML/CFT training (including details of content and completion) are to be kept in the HR system as part of their CPD record keeping

Staff are to advise the Compliance Officer of all AML/CFT related training they have undertaken.

All training must be CPD compliant (as per the NZ Law Society guideline) as this sets the threshold for quality, the Compliance Officer reserves the right to reject training they consider substandard.

The Compliance Officer is to approve the use of any third-party vetting agents. The use of vetting agents must be in line with the above requirements and assessed and managed using the 'Institutions' section of the firm's Risk Assessment and 'Employee Due Diligence' section of the Internal Controls Report.

The Reporting Officer is to consider 'Trigger Events' that would require additional training to be completed by staff and partners. These would include (but are not limited to):

- material changes to the Act or the Compliance Programme
- new staff starting work
- staff and partners changing roles or newly undertaking captured activities
- evidence of staff not complying with the Act or the Compliance Programme
- the firm offering new services or products that are captured by the Act

15.0 Audits, Annual Reporting and Record Keeping

15.0 Audits

Internal spot audits will be completed (as per section 10.6 of this document). This Compliance Programme and the AML/CFT Risk Assessment must be reviewed and audited by an independent and appropriately qualified person every three years or at any time at the request of the AML/CFT supervisor.

The Compliance Officer is approved to select the independent auditor and is responsible for ensuring the audit requirements are adhered to.

15.1 Annual Reporting

The firm is required to submit an annual AML/CFT report confirming compliance with the AML/CFT Act and provide the information requested.

Staff and partners need to be aware of the client-related data required for the report. They must ensure it is correctly captured and entered into the practice management system.

The Compliance Officer is approved to submit the report and is responsible for ensuring the information requirements of the annual report are adhered to.

The report is to be submitted online using the AML Online website/portal.

15.2 Compliance Programme Breaches

Any breaches of processes and procedures detailed in this document or the AML/CFT Act must immediately be reported to the Compliance Officer. Breaches may be detected by internal checks, general observations, or independent audits. All breaches are to be thoroughly investigated and depending on severity may result in:

- increased staff training obligations
- increased monitoring or spot audits
- disciplinary proceedings
- staff dismissal
- review of the Risk Assessment and Compliance Programme
- other actions considered appropriate by the Compliance Officer and/or Partner to reduce the risk of the breach reoccurring

15.3 Record Keeping

All client documents including AML/CFT and CDD related information is to be kept electronically within our practice management systems Action Step and Spinika for a five-year period. It is Tompkins Wake's standard procedure to keep all client documents for a minimum of ten years. Information must be retained so that you can readily reconstruct transactions or activities, as well as ongoing business relationships. Such information includes:

- information on the nature and purpose of the business relationship
- customer due diligence information
- any forms or file notes
- records of activities such as phone calls, letters, notes on meetings and conversations
- risk assessments, compliance programmes, audits, and other updates to AML/CFT documentation
- any other information relevant to the services you provide to your clients.

The starting point for the five years is after the completion of the matter/activity or end of the business relationship.

The internal spot audits required as per section 10.6 are used to ensure records are kept in accordance with the above requirements. The firm's own internal record destruction policies must not conflict with the above requirements and should ensure appropriate destruction measures are in place. When information is kept for the purposes of the AML/CFT Act, the record is to be destroyed as soon as practicable after the retention period has expired.

15.4 Information Storage

AML/CFT records may be kept in either hard copy or electronically. They must be stored in a way that enables production:

- to a supervisor
- to law enforcement
- for audit purposes

All CDD information and forms are to be scanned and linked to the client's records using the AML management system (Spinika). CDD information is relevant to clients who are individuals and multiple individuals may need to be identified for some clients.

Ensure all new matters are opened and categorised correctly in line with Tompkins Wake's practice management system processes. This is essential to ensure Tompkins Wake meets its CDD obligations and ongoing reporting and audit requirements.

16.0 Wire Transfers

Effective 31 July 2023, new Regulation 15A of the AML/CFT (Definitions) Regulations 2011 exempts all designated non-financial business or profession (DNFBPs) that make or receive wire transfers from or into their trust accounts from being an ordering, an intermediary, or a beneficiary institution of a wire transfer. This applies to us and includes both domestic and international wire transfers.

This exemption does not apply to the firms' obligations to make PTR's or undertake CDD on clients for whom we hold funds. It applies to the information gathering and traceability requirements set out in section 22(3) and sections 27-28 of the Act.

You must complete CDD on your client before making any funds available to them or using the funds for a transaction.

Trust account operating procedures need to ensure the above requirements and those contained within section 10.2 are being met and monitored. These are to be tested and reported in the "Internal Controls Report" under the section named "Trust account monitoring being undertaken and appropriate."

17.0 Reassessment Criteria and Process

This Compliance Programme is to be approved by the Board.

The Board authorises the AML Compliance Officer to alter, modify or vary the Compliance Programme with minor changes that are deemed necessary or desirable to improve the firm's AML processes. Changes can be made during the twelve-month review period and then presented to the Board annually.

This Compliance Programme is to be updated/reviewed if any of the following events occur:

- it has been more than 12 months since the last update/review
- a new 'Risk Statement' is issued by the Board
- there have been relevant changes to the AML/CFT Act or guidance issued by the supervisor
- there has been a known material breach of the Compliance Programme
- new products, services or delivery channels are to be offered to clients
- any areas of practice are known to have experienced material increased risk
- the firm decides to approve a third-party agent(s) to regularly conduct CDD on their behalf (including electronic identity verification providers).
- such a request has been made or recommended by an auditor or the supervisors.

Any changes/reviews of this Compliance Programme are to be recorded below.

Date	Version No.	Reason for Review/Change	Approved By	New Version
30 June 2018	n/a	Initial Compliance Programme	Board of Partners	V1
31 March 2021	V1	Review and update based on the independent auditor's report and AML Assist recommendations (all accepted).	Board of Partners	V2
15 December 2021	V2	Review and update of changes made by Compliance Officer	Board of Partners	V3

8 June 2022	V3	Removal of the requirement for 24-month reverifying of client identification, the adoption of First AML as third party provider, the new AML role in the firm, authorisation for the AMLCO to make minor changes to the Compliance Programme and addition of Russian sanctions to the country risk assessment.	Board of Partners	V4

21st January 2023	V4	Update EIV Providers, add matter risk assessment to CDD processes, update training processes, reporting officer's role, captured activities table and work codes. Additions to verifications for company nominee directors/shareholders and limited partnerships with nominee general partners. Update estate processes for executor/administrators, add formal PEP checks and additions to SOW, simplified and ongoing CDD. Removal of the AML Committee. Add the Delayed due diligence process. Other minor corrections.	Board of Partners	V5
06 March 2024	V5	Review and redocumentation to reflect new AML processes incorporating Spinika with Action Step and AML Assist recommendations. Includes the Act amendments that came into effect 31 July 2023. SCDD processes updated to reflect class exemption that came into effect 31 December 2023.	Board of Partners	V6
30 June 2024	V6	Updated to reflect the Act changes that came into effect in June 2024 and minor corrections.	Board of Partners	V7
31 July 2024	V7	Updated to reflect the Act changes that came into effect in June 2024 and the updated guidance material released by the DIA	Board of Partners	V8

Appendix A – Acceptable ID (Individuals)

Photographic ID – Any One

Staff can obtain and rely upon one of the following forms of primary photographic identification:

- New Zealand passport – valid for two years from expiry unless another passport has been issued
- New Zealand certificate of identity
- New Zealand refugee travel document
- Emergency travel document
- New Zealand firearm's licence
- Overseas passport or a similar document issued for the purpose of international travel that contains: the name, date of birth, a photograph, and the signature of the person in whose name the document is issued; and is issued by a foreign government, the United Nations or an agency of the United Nations
- A national identity card issued for the purpose of identification, that contains: the name, date of birth and a photograph of the person in whose name the document is issued and their signature; and is issued by a foreign government, the United Nations, or an agency of the United Nations (an overseas driver's licence does not meet this requirement)

NZ Driver Licence – ID Combinations

Staff can obtain a New Zealand driver licence in combination with a secondary or supporting form of identification:

- NZ Defence Photo ID
- Police Photo ID
- A document issued by a registered bank that contains the person's name and signature – for example an embossed eftpos card. The card must be issued by a registered bank in NZ or a reputable bank operating in a low-risk jurisdiction. Note the card should have account numbers and security code redacted prior to being saved into Spinika.
- A bank statement or letter issued by a registered bank to the person in the last 12 months. The statement must be issued by a registered bank in NZ or a low-risk jurisdiction

- A document issued by a government agency that contains the person's name and signature, for example a SuperGold Card or Community Services Card. Note: staff may accept a community services card if the client offers it, however they cannot request it
- A statement issued by a government agency to the person in the last 12 months
- Electronic identity verification from any firm-approved service provider
- Confirmation that the information presented on the driver licence is consistent with records held in the National Register of driver licences
- Confirmation that the information presented on the driver licence is consistent with records held by a reliable and independent source.

Non-Photographic ID – Combinations

Staff can obtain one of the following forms of primary non-photographic identification:

- New Zealand full birth certificate
- Certificate of New Zealand citizenship
- Citizenship certificate issued by a foreign government
- Birth certificate issued by a foreign government, the United Nations, or an agency of the United Nations.

The above must be in combination with a secondary or supporting form of photographic identification:

- New Zealand driver licence
- NZ Kiwi Access (18+) Card (Hospitality Association)
- NZ Defence Photo ID
- Police Photo ID
- Valid and current international driving permit.
- Other photographic identification considered independent and reliable that has been approved by the Compliance Officer.

For clients under 18 years of age, a full New Zealand birth certificate can be accepted as sole identity but only if no other identity methods can be met.

Conditions of Identification

All documents provided for identification purposes must be:

- original documents
- clear, legible, a good likeness, not defaced, mutilated, or tampered with
- valid (signed and not cancelled)
- sighted by staff or a trusted referee
- translated to English by the client, staff or a trusted referee.

Warning - Collection of Identification

Caution is required when collecting and storing the private information of our clients. Consideration must be given to:

- compliance with our privacy processes and Privacy Act requirements
- ensuring any debit card or other information is not retained in a form that would allow it to be used in a fraudulent manner (account and security code information must be redacted)
- ensuring personal information contained within a birth certificate is redacted if requested (i.e. parents names, place of birth or sex assigned at birth).

Appendix B – Acceptable Address Verification

The following documents are acceptable for individuals:

- Utility bill
- Rates bill
- Bank account statement or Bank confirmation letter; must be issued by registered bank in NZ or low risk jurisdiction
- Insurance policy document
- Car registration notification/demand
- IRD tax notice/certificate
- Non-bank financial institution statement (excludes financial advisers, mortgage brokers, money remitters etc.)
- Sale's Notice, provided the LTTS confirms 'main home transfer" (question 3B) removed
- Electronic yellow pages (staff member to check and verify address)
- Electronic white pages (staff member to check and verify address)
- An approved third-party electronic identity verification provider
- Rental tenancy agreement
- A letter from their current employer
- Companies Office records for existing clients (i.e. confirms an address already held in your system)
- Electoral roll papers
- Government, government department or government agency document
- Local Council notification or demand
- Court document
- NZQA registered education provider. A letter from educational facility must be on their letterhead paper and signed by a principal
- Minors - parent/ guardian verification that includes (a) matching a parent's name on the birth certificate to that parents address verification; or (b) a letter (or in person) from a

parent/ guardian and parent/ guardian address verification

- The following address verification options are acceptable for migrants, international visitors, and students only when the above requirements cannot be met:
    - A letter from the client's host accompanied by verification of the host's address
    - A letter from an employer when the employer owns the property where the client resides
    - Confirmation of short-term accommodation from an accommodation provider (i.e. invoice, receipt, letter)
    - Letter from the holder of the tenancy agreement, where client is not on the tenancy agreement
    - Overseas equivalent of a Utility bill or rates bill showing their overseas residential address.

Conditions of Identification

All documents provided for identification purposes must:

- display the client's name and residential address
- be dated within the last 3 months for new clients, and 12 months for ongoing clients
- not be targeted promotional or marketing material
- be clear and legible
- valid (signed and not cancelled)
- sighted by staff or a trusted referee or considered original source*
- translated to English by the client, staff, or a trusted referee.

Documents can be originals or official online versions. This excludes NZ Drivers Licence and NZ Electoral Office documents.

** Original source documents would include documents signed by the issuer as true copies of the original or a confirmation of information held within their records. It could also include the above documents that have been emailed directly to clients that have then been forwarded to the firm, provided the staff member is confident the email has come directly from the original source and has not been tampered with or altered in anyway.*

Appendix C – Acceptable ID (Entities)

Legal Entity Verification

Staff can obtain and verify one of the following forms of identification:

- New Zealand Companies Office – Official extracts
- NZX or other Recognised Exchange – Official extracts
- Certificate of Incorporation
- Trust Deed (current and with all supporting documentation)
- Partnership Agreement (current and with all supporting documentation)
- Club or Society constitutional documents or meeting minutes if unincorporated
- Foundation Document (current and with all supporting documentation)
- Limited partnership agreement for non-New Zealand and non-registered Limited Partnerships (current and with all supporting documentation)
- Legislation forming the Government entity
- Government website
- Relevant website confirming Government entity status
- Regulator in a low-risk jurisdiction
- Overseas Companies Registry
- Audited Financials (if the sources above cannot be supplied).

Legal Entity Address Verification

Staff can obtain and verify one of the following forms of identification:

- New Zealand Companies Office – Official extracts
- Charities Commission - Official extracts
- NZX or other Recognised Exchange – Official extracts
- Partnership/ Limited partnership agreement

- Trust Deed
- Audited Financials
- Utility bill (online statements may be accepted provided the clients address is the same address of the services relating to the utility bill)
- Rates bill (online statements may be accepted provided the clients address is the same address of the property that the rates bill applies to)
- Bank account statement
- IRD tax notice/ certificate
- Board resolution or minutes of a meeting (for informal entities only)
- Constitutional documents
- Regulator in a low-risk jurisdiction - Official extracts
- Overseas companies registry - Official extracts
- Government website - Official extracts

Appendix D – Source of Wealth and Funds

When conducting ECDD, staff must take reasonable steps, according to the level of risk, to verify the source of wealth and funds. Source of wealth are the activities that created the total net worth of the client. Source of funds includes the origin and means of transfer for any funds that are to be used in the client matter/transaction. For client five year's plus, see the practice management system precedents for the SOW/SOF file note, otherwise discuss with your client how their source of wealth was acquired and obtain evidence of this.

Staff must obtain and verify at least one of the following:

- Copy of pay slips from the last 3-6 months
- Bank statements from the last 3-6 months
- IRD documents, such as tax returns
- Audited financial statements or accountant prepared financial statements certified by an accountant
- Copy of the sale contract for the sale of any property, shares or other assets
- Letter from a donor making a gift along with confirmation of the donor's source of wealth (as set out in this document).
- Confirmation from the Lotteries Commission or a regulated betting agency confirming the win
- Copy of insurance company statement confirming proceeds
- Letter from insurance company confirming surrender/withdrawal of proceeds
- Copy of superannuation providers statement confirming proceeds
- Letter from superannuation providers confirming withdrawal of proceeds
- Copy of statement confirming proceeds held in any investment funds
- Letter from a regulated provider of investment fund services
- Letter from superannuation providers confirming withdrawal of proceeds
- Letter from solicitor or accountant verifying source of wealth.
- Letter from accountant for Tompkins Wake longstanding clients.

Staff should also make their own enquires that could include:

- internet research
- information provided by trusted intermediaries
- reliable media sources
- publicly available databases
- professional third-party providers of such information.

Staff must develop an understanding of the size and nature of the client's wealth and how it was acquired.

Appendix E – Acceptable Certifiers

If the client is unable to complete CDD face-to-face, they can choose to have the above identification and address verification documents verified by a successful EIV process or certified by an approved trusted referee, provided the following procedures are followed:

- Certification must have occurred within the past three months.
- Certification must include the name, occupation and signature of the certifier and the date of certification.
- Certification of identity documentation must include a statement that the document represents a true likeness of the individual being identified
- The certifier must be at least 16 years of age and cannot be one of the following:
    - related to the client i.e. a parent, child, brother, sister, aunt, uncle, cousin
    - the spouse or partner of the client
    - a person who lives at the same address as the client
    - a person involved in the transaction or business requiring certification

NZ Trusted Referees

- Member of the police
- Justice of the peace
- Registered medical doctor
- Kaumatua (as verified through a reputable source)
- Registered teacher
- Minister of religion
- Lawyer
- Notary public
- New Zealand Honorary Consul
- Member of Parliament
- Chartered accountant
- A person with the legal authority to take statutory declarations.

Overseas Trusted Referees

If the client is unable to complete CDD within New Zealand, they can choose to have the identification and address verification documents (listed above) certified by an acceptable trusted referee in their country of residence.

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

Where possible, it is expected the staff member will locate a reference as to who can take a statutory declaration on the applicable government website of the respective country. Alternatively, staff may rely on an agent duly authorised by the Compliance Officer to act on behalf of the firm.

It is expected that the overseas trusted referees will hold roles similar to New Zealand trusted referees and rely on the same types of documentation mentioned above herein to verify the client and provide certification. They must specify their capacity to act as a trusted referee and meet the requirements detailed above.

Extra care must be taken in high-risk jurisdictions and all such cases should be referred to the Compliance Officer.

Appendix F – SCDD Client Qualification

The following clients qualify for simplified client due diligence:

- Listed on an authorised stock exchange
- Reporting entities supervised or regulated under the NZ AML/CFT Act and licensed or regulated in accordance with the Insurance (Prudential Supervision) Act 2010 and the Reserve Bank of New Zealand Act 1989
- Government departments named in Schedule 1 of the State Sector Act 1988
- Local authorities as defined in section 5 of the Local Government Act 2002
- New Zealand Police
- New Zealand Security Intelligence Service
- Licensed supervisor or statutory supervisor under the Financial Markets Supervisors Act 2011
- Trustee corporations, within the meaning of section 2(1) of the Administration Act 1969
- Crown entities, as defined in section 7(1) of the Crown Entities Act 2004
- an authorised agent named in Schedule 4 of the Public Finance Act 1989
- Licensed managing intermediaries, within the meaning AML/CFT Act which include:
    - licensed non-bank deposit takers;
    - licensed managed investment schemes;
    - Financial Markets Conduct Act 2013 licence holders;
    - Financial Markets Authority appointees;
    - registered managed investment schemes;
    - certain unit trust, KiwiSaver and superannuation schemes.
- Specified managing intermediary, within the meaning AML/CFT Act which include:
    - a financial institution supervised or regulated under the NZ AML/CFT Act;
    - a foreign financial institution.
- Government bodies located in a low-risk jurisdiction that:
    - corresponds to a government department named in Schedule 1 of the State Sector Act 1988; and
    - is located in an overseas jurisdiction with sufficient anti-money laundering and countering financing of terrorism systems and measures in place

Appendix G – Recognised Stock Exchanges

An authorised stock exchange is:

- a stock exchange or securities exchange where stockbrokers and traders can buy and sell securities, such as shares of stock and bonds and other financial instruments, and
- registered in a country with sufficient disclosure requirements and sufficient AML/CFT systems in place.

The companies' equity securities must be listed on a recognised stock exchange to quality for SCDD, otherwise normal CDD procedures must be applied.

Below is a link to a list of global stock exchanges. To be a recognised stock exchange a country risk assessment must also be completed (as per appendix H) and considered Low Risk.

Sites that list global stock exchanges:

- https://www.tradinghours.com/markets
- https://en.wikipedia.org/wiki/List_of_stock_exchanges
- https://tradingeconomics.com/stocks
- https://www.bloomberg.com/markets/stocks

Appendix H – Country Risk Assessment

The firm has chosen to use a selection of resources including the list of FATF countries for assessing country jurisdiction risk.

These resources are:

- Jurisdictions under Increased Monitoring - June 2022 (fatf-gafi.org)
- UN sanctions | New Zealand Ministry of Foreign Affairs and Trade (mfat.govt.nz)
- Global Terrorism Index | Countries most impacted by terrorism (visionofhumanity.org)
- Tax Haven Countries 2023 (worldpopulationreview.com)
- 2021 Corruption Perceptions Index - Explore… - Transparency.org
- Glossary:List of offshore financial centres - Statistics Explained (europa.eu)

Jurisdictions under increased monitoring (due to strategic deficiencies) by FATF are, Bulgaria, Burkina Faso, Cameroon, Croatia, Democratic Republic of the Congo, Haiti, Jamaica, Kenya, Mali, Monaco, Mozambique, Namibia, Nigeria, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Türkiye, Venezuela, Vietnam, and Yemen.

Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the “grey list”. High-risk jurisdictions subject to a Call for Action (due to strategic deficiencies) include Democratic People’s Republic of Korea (DPRK), Iran and Myanmar.

The Russia Sanctions Act 2022 and Russia Sanctions Regulations 2022 prohibit dealing with assets and services of sanctioned persons and classes of persons and should be considered as part of the jurisdiction risk. There is also a duty for a reporting entity that is in possession or in immediate control of assets that it suspects are designated assets or assets owned or controlled by a designated person, to report these suspicions to the Commissioner no later than 3 working days.

Secondary resources can be used to assist with country risk assessment, these include publications from other Authorised AML/CFT service providers. An example of such a secondary resource is “The Basel Index Report” https://index.baselgovernance.org or Know your country reports https://www.knowyourcountry.com/country-reports/.

The firm has no standing approvals for country risk and this risk should be reassessed with every new client, beneficial owner and transaction/activity. Material changes provisions also apply should a client’s association with a country change or country risk increases.

Appendix I – Technical References

This Compliance Programme has been purposely formatted in a "Plain English" style to make it easy for staff to read and follow. Its layout does not follow a traditional format with headings of policy, procedure and control however these have been embedded into the documentation as required by the act.

Below we have detailed how this Compliance Programme adheres to the requirements of the act by providing cross references between this Compliance Programme and the requirements of the AML/CFT act.

Risk assessment considerations

Section 57(1) of the Act requires CDD to be risk based and reflect the risk assessment

Policy	Compliance Programme is to address the key risks identified in the Risk Assessment.
Procedure	Section 1.0 Introduction and Section 2.0 Risk Assessment
Control	Section 17.0 Reassessment Criteria. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Employee due diligence

Section 57(1)(a) requires adequate and effective procedures, policies, and controls for vetting senior managers, the compliance officer and any other employee that is engaged in AML/CFT activities.

Policy	All new employees undertaking captured activities are to be vetted
Procedure	Section 13.0 Employee Due Diligence
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Staff training

Section 57(1)(b) requires adequate and effective procedures, policies, and controls for training senior managers, the AML/CFT compliance officer and any other employee that is engaged in AML/CFT duties.

Policy	All employees undertaking captured activities are to be trained.
Procedure	Section 14.0 Training Requirements.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Staff Training Register.

Client due diligence requirements

Section 11 and 57(1)(c) of the Act requires processes to identify and verify the client, any beneficial owner of a customer and any person acting on behalf of a customer before conducting an occasional transaction or activity or establishing a business relationship.

Section 57(1)(j) of the Act requires procedures to determine whether a lower standard of Simplified CDD can be permitted and when a higher standard of enhanced CDD is required.

Policy	CDD to be completed on all clients undertaking captured activities.
Procedure	Section 5.0 Types of CDD. Section 6.0 Client Identification and Verification. Section 7.0 Standard CDD. Section 8.0 Enhanced CDD. Section 9.0 Simplified CDD.
Control	Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

CDD alignment with IVCOP

Unless an "opt out" has been approved CDD needs to be completed in compliance with the Identity Verification Code of Practice 2013 (IVCOP).

Policy	The firm has adopted the IVCOP.

Procedure	CDD processes throughout the Compliance Programme (and appendices) are based on the IVCOP standards.
Control	Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Captured & occasional activities/transactions

Section 5(1) and 6(4)(a)-(e) of the act defines the activities captured by the Act. Section 57(1)(c) requires CDD also be conducted on occasional activities or occasional transactions

Policy	The firm is to understand all captured activities it undertakes and apply the Compliance Programme in these instances.
Procedure	Section 4.0 Captured Activities.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Guidance material understood

Section 57(1)(2) of the Act requires that the compliance programme has regard to guidance material produced by DIA and the Police Financial Intelligence Unit relating to the compliance programme.

Policy	The Compliance Officer will be primarily responsible for staying informed on all guidance material.
Procedure	Section 1.0 Introduction. Section 14.0 Training Requirements.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Staff Training Register.

Compliance officer appointment

Section 56(2)-(4) of the Act requires the appointment of an AML/CFT compliance officer to administer and maintain its AML/CFT programme.

Policy	The Compliance Officer is to be selected and appointed by senior

	management.
Procedure	Section 3.0 Compliance Officer Selection.
Control	Not applicable. Policy applies when any changes to the role occur.

Ongoing CDD & monitoring

Section 31 and 57(1)(c) of the Act requires adequate and effective procedures, policies and controls for account monitoring and conducting ongoing customer due diligence.

Policy	The firm and staff will conduct appropriate monitoring and ongoing CDD on our clients as required.
Procedure	Section 10.0 Ongoing CDD. Section 14.0 Training Requirements.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Staff Training Register.

Annual report, audit, SAR and PTR's

Section 57(1) requires adequate and effective procedures, policies, and controls for identifying and reporting suspicious activities and reporting cash transaction valued at NZ$10,000 or over, and for any international wire transfer valued at NZ$1,000 or over.
Section 59 requires the appointment of an independent auditor every 3 years. Section 60 requires the preparation of an annual report as directed by the supervisor.

Policy	The firm will ensure all reporting and audit requirements are met.
Procedure	Section 11.0 Assessing Risk and Red Flags. Section 12.0 Reporting Suspicious Activity and Transactions. Section 15.0 Audits, Annual Reporting and Record Keeping.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Record keeping

Section 57(1)(e) of the Act requires that records are retained on client's identity and the documents that were used to verify it, as well as records to enable any transaction carried out to be fully reconstructed at any time.

Policy	All relevant AML/CFT documents and records will be kept for 5 years.
Procedure	Section 15.0 Audits, Annual Reporting and Record Keeping.

Control	Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Enhanced client due diligence & written findings

Section s22-25 and 57(1)(c) of the Act requires that a reporting entity obtain and verify information relating to the source of funds or the wealth of the customer.

Section 57(1)(g) of the Act requires effective procedures, policies and controls for monitoring, examining and keeping written findings relating to; complex or unusually large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose, and any other activity that the reporting entity regards as being particularly likely by its nature to be related to money laundering or financing of terrorism.

Policy	Enhanced CDD will be untaken when prescribed by the act and also whenever potential ML/FT risks are identified.
Procedure	Section 8.0 Enhanced CDD. Section 10.2 Trust Account Transaction Monitoring. Section 11.0 Assessing Risk and Red Flags. Appendix D Source of Wealth and Funds.
Control	Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Red Flag Checklist. ECDD File Note Form (the format used to record written findings)

Nature, purpose and material change

Section 17 and 25 of the Act requires the collection of information on the nature and purpose of the business relationship. Section 14(1)(c) requires the provision for CDD to be completed on existing clients where there has been a material change.

Policy	Staff are to be trained to assess nature and purpose of their client relationships. CDD is to be completed on all existing client where a material change has occurred.
Procedure	Section 6.1 Client Identification. Section 6.0 Client Identification and Verification. Section 7.0 Standard CDD. Section 8.0 Enhanced CDD. Section 9.0 Simplified CDD. 7.0 Section 10.3 Trigger Events and Material Change Reviews. Section 14.0 Training Requirements.
Control	Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit

	Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Politically exposed persons

Section 26 and 57(1)(c) of the Act requires that reasonable steps are taken to determine whether the customer or a beneficial owner is a Politically Exposed Person (PEP).

Policy	Staff must consider and understand how to identify any PEPs, their close associates and close family members.
Procedure	Section 8.6 Politically Exposed Person. Section 10.5 High and Extreme Risk Client Reviews.
Control	Red Flag Checklist. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report.

Country risk

Section 57(1)(h) of the act requires adequate and effective procedures, policies, and controls for monitoring, examining and keeping written findings relating to business relationships and transactions from or in countries that do not have or have insufficient AML/CFT systems in place.

Policy	Country Risk is to be assessed and considered for all clients undertaking captured activities.
Procedure	Section 8.0 Enhanced CDD. Section 8.3 Written Findings, Escalation and Approval Processes. Section 10.5 High and Extreme Risk Client Reviews. Section 11.0 Assessing Risk and Red Flags. Appendix H Country Risk Assessment.
Control	Red Flag Checklist. Section 10.6 Internal Spot Audits. Internal Spot Audit Form. Internal Spot Audit Register. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. ECDD File Note Form.

Verification

Section 57(1)(c)-(k) of the Act allows reliance on third parties, including agents, to conduct CDD procedures on their behalf. Adequate and effective procedures, policies and controls are required.

Policy	The Compliance Officer has the authority to approve the use of third parties.
Procedure	Section 6.3 Identifying an Owner's Agent. Section 6.6 Electronic Identity Verification.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Section 10.6 Internal Spot Audits. Internal Spot Audit Form. EIV Provider Assessment and Approval Form

Prohibitions and exceptions

Sections 37, 38 and 39 provides details on prohibitions for certain circumstances and client types. The IVCOP requires appropriate exception handling procedures for circumstances when a client demonstrates that they are unable to satisfy the requirements of the code.

Policy	The firm will not engage any prohibited/extreme risk clients. Staff can submit any CDD exceptions to the firm's authorised approvers.
Procedure	Section 6.8 Verification Exception Handling. Section 8.3 Escalation and Approval Processes. Section 11.0 Assessing Risk and Reg Flags.
Control	Verification Exception Approval Form. Red Flag Checklist. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report

Wire transfers and trust account

Section 27-28 of the Act requires provisions are in place for any wire transfers (over a threshold) are made or received on behalf of clients.

Policy	The firm will ensure the required information is obtained and CDD completed on all wire transfers over $1,000.
Procedure	Section 16.0 Wire Transfers
Control	Section 10.2 Trust Account Transaction Monitoring. Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report

New technologies and anonymity

Section 57(1)(i) of the Act require adequate and effective procedures, policies, and controls for mitigating and managing the ML/FT risk of new or developing technology, or new or developing products, that may favour anonymity.

Policy	The firm will undertake ECDD on any client that has new or developing technology, or new or developing products, that may favour anonymity.
Procedure	Section 8.1 Criteria for ECDD. Section 8.7 Technologies, Products, Services or Delivery Channels - Favour Anonymity. Section 11.0 Assessing Risk and Red Flags.
Control	Section 2.1 Managing and Mitigating ML/FT Risks. Internal Controls Report. Red Flag Checklist. ECDD File Note Form.

Managing and mitigating risk

Section 57(1)(l) of the Act requires adequate and effective procedures, policies and controls for monitoring and managing compliance with its AML/CFT programme.
Section 59(1) of the Act requires review of the compliance programme in order to ensure it remains current and to remedy any deficiencies in effectiveness.

Policy	The firm's Compliance Officer will be primarily responsible for managing and mitigating risks.
Procedure	Section 2.1 Managing and Mitigating ML/FT Risks. Section 17.0 Assessment Criteria and Process.
Control	Internal Controls Report. Section 3.0 Compliance Officer Section (reporting to senior management)

Appendix J – Abbreviations and Acronyms

Term	Meaning
AML/CFT	Anti-money laundering and countering financing of terrorism
The Act	AML/CFT Act 2009
The firm	Tompkins Wake
ActionStep	The firm's practice management system
Spinika	Firms AML/CFT management system
Client	The client and any beneficial owner
Client Matter	The activity being undertaken as recorded in ActionStep
Compliance Officer	AML/CFT Compliance Officer (AMLCO)
CDD	Client due diligence
CPD	Continued Professional Development
DIA	Department of Internal Affairs
ECDD	Enhanced client due diligence
SCDD	Simplified client due diligence
OCDD	Ongoing client due diligence
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
ML	Money laundering
PEP	Politically exposed person
POA	Power of Attorney
Compliance programme	AML/CFT programme
Risk assessment	AML/CFT risk assessment
SAR	Suspicious activity report
STR	Suspicious transaction report
FT	Financing of Terrorism
NZX	New Zealand Stock Exchange

CEO	Chief Executive Officer
Red Flags	Possible ML/FT risk identifiers
Spot Audit	Internal compliance check
ID	Identification
EIV	Electronic Identity Verification

Appendix K – Actionstep Matter and Sub Matter Types

MATTER TYPE	SUB TYPES	CDD Required?
Civil	Litigation	N & Y[1]
	Local Authority – Litigation	N & Y
	Local Authority – Advisory	N
	Advice Only - Civil	N
Commercial	Mergers and Acquisitions	Y
	Company Formation or Restructuring	Y
	Shareholder Arrangements	Y
	Capital Raising Matters	Y
	Directorship/Governance Matters	N[2]
	Commercial Contracts	N
	Partnership Arrangements	Y
	Privacy Matters	N
	Other Corporate or Commercial Matters	Y/N
	Advice Only - Commercial	N
Conveyancing - Purchase	Residential - Conveyancing Purchase	Y
	Rural - Conveyancing Purchase	Y
	Commercial - Conveyancing Purchase	Y
Conveyancing - Sale	Residential - Conveyancing Sale	Y
	Rural - Conveyancing Sale	Y
	Commercial - Conveyancing Sale	Y

[1] Litigation that leads to management settlement proceeds via trust account will require CDD

[2] Advice only – for example changes in Directors would fall under Company Formation and be captured

Employment	Employment Disputes	Y & N[3]
	Health and Safety	N
	Employment Agreements and Policy	N
	Local Authority	N
	Advice Only - Employment	N
Environmental & Resource Management	Private Client	N
	Local Authority - Resource Consent or Designation in Regulatory Role	N/Y
	Local Authority - Plan Review, Plan Change or Private Plan Change Request	N
	Local Authority - Enforcement and Prosecutions	N
	Local Authority - As Applicant or Requiring Authority	N
	Local Authority - General Advice	N
Estate Administration	Estate Administration	Y
Family	Reproductive	N
	Family Legal Aid	N
	RPA, Contracting Out	N
	Advice Only - Family	N
	Lawyer for Child	N
	Capacity – PPPR	N
	Trust and Will Disputes	Y/N[4]
	Relationship Property	N[5]
	Spousal maintenance	N
	Section 182 claims	N
	Contracting Out	N
	Dissolution	N

[3] Employment matters that lead to a settlement via trust account will require CDD

[4] Only captured where a dispute leads to a settlement via trust account

[5] Where a Relationship Property matter leads to a captured activity a separate matter should be opened to deal with any conveyancing or settlements via trust account.

	Care of Children	N
	Family Violence	N
	Adoption	N
	Estate Claims	Y
	Surrogacy	N
Finance	Refinancing	Y
Immigration	Advice Only - Immigration	N
	Application to INZ – visitor	N
	Application to INZ - student	N
	Application to INZ – work	N
	Application to INZ – residence	N
	Application to INZ – family	N
	Application to INZ – section 61	N
	Application to INZ – employer	N
	Application to INZ - investor	N
	Application to INZ – other	N
	Appeal to IPT	N
	Request to Minister	N
	MBIE proceedings	N
	Citizenship application	N
	Deportation defence	N
Intellectual Property	Applications	N
	Renewals	N
	Disputes	N
	Commercial	Y & N[6]
	Advice Only - Intellectual Property	N
Lease	Advice Only - Lease	N
Notary Public	Notary Public	N

[6] Sale or Purchase of IP would be captured

Property	Advice Only - Property	N
	Property – Easements	N/Y
	Property Development	Y
	Property – Local Authority	Y
	Environmental	N
	Leases – Leasehold interests	Y[7]
	Property – Licences	Y
Retirement Villages/ORA	Advice Only - Retirement Villages	N
	Sale	Y
	Purchase	Y
	Disputes	Y/N
Sale - Rangitahi Limited	Sale - Rangitahi Limited	Y/N
Stage Three/Four Transfer	Stage Three/Four Transfer	Y/N
Subdivision	Subdivision	Y
Third Party Easements	Third Party Easements[8]	N/Y
Trust Formation and/or Estate Planning	Wills/Codicils/EPOA's	N
	Trust Formation	Y
	Charitable Trust Formation	Y
	Asset Planning	Y
Trust Matters	Change of Trustees	Y
	Winding Up	Y
	Removal/Appointment of Beneficiaries	Y
	Trust Administration	Y

[7] Commercial leasing is recognised as an area of ML/TF risk and is therefore captured. Persons engaged in work to negotiate and transact a commercial lease are providing real estate work and subject to the full range of AML obligations.
[8] Securing an obligation is not captured. Sales and purchase of land would be captured.

	Variation/Power of Appointment	Y
Whangamoa Lease Transfer	Whangamoa Lease Transfer	Y/N