Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Guideline:

Lawyers and Conveyancers

Complying with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

December 2017

Contents

Executive summary

It is likely that money laundering is currently going undetected in New Zealand. Money laundering is the method by which people disguise the illegal origins of the proceeds of crime and protect and enjoy their assets. Some people in New Zealand may also be financing the activities of terrorists and known terrorist organisations. Financers of terrorism use similar techniques to money launderers to avoid detection by authorities and to protect the identity of those providing and receiving the funds.

People with criminal intentions value anonymity and are looking for ways to distance themselves from their activities while still enjoying the proceeds of their crime. Both domestic and international evidence suggests that using gatekeepers, such as lawyers and conveyancers, is a way for criminals to create a false perception of legitimately acquired wealth. The recent changes to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act or the Act) included lawyers and conveyancers in the AML/CFT system.[1]

The AML/CFT Act is activities-based. Only lawyers and conveyancers who undertake specified activities will need to develop a programme to ensure they comply with the requirements in the Act. The flow chart on page 8 of this guideline can help you determine if you are captured by the AML/CFT Act.

You must comply with the AML/CFT Act by ensuring you identify, understand and can assess the risks of money laundering and terrorist financing (ML/TF) to your business, and by implementing an AML/CFT programme to manage those risks. AML/CFT programmes will vary from business to business according to each management's judgement about how to best manage the specific risks they have assessed. This guideline provides a summary of what businesses must include in their AML/CFT programme to ensure they comply with the Act.

Lawyers and conveyancers need to know their customers. Before conducting captured activities, they need to conduct customer due diligence (CDD) according to the level of risk posed by their customers. CDD is not optional.

When lawyers or conveyancers are not able to complete CDD, they must not undertake a captured activity or transaction for that customer. To do so would be a breach of the AML/CFT Act.

The Department of Internal Affairs (DIA) is the supervisor charged with monitoring lawyers' and conveyancers' compliance with the AML/CFT Act. We recognise that adjusting to the new AML/CFT system will take time and effort. Lawyers will have the additional task of ensuring they uphold legal professional privilege. This guideline, and other existing guidelines, can help law firms, conveyancing practitioners and incorporated conveyancing firms to develop robust awareness of the risks posed by ML/TF and provide prompts on what to think about when developing programmes to manage these risks. We are available to respond to queries, and we are working with professional bodies in the legal and conveyancing sectors to ensure that the sectors are well supported to meet their obligations under the AML/CFT Act.

Disclaimer

This guideline is provided for information only and cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It does not constitute legal advice and cannot be relied on as such. After reading this guideline, if you do not fully understand your obligations you should seek legal advice or contact your AML/CFT supervisor. DIA can be contacted at amlphase2@dia.govt.nz.

Glossary

AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
AML/CFT Amendment Act	Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2017
Captured activities	Activities that are specified under the definition of "designated non-financial business or profession" in the AML/CFT Act
CDD	Customer due diligence
Compliance officer	An individual (usually an employee) appointed to administer and maintain the AML/CFT compliance programme
Customers/Clients	While the term "clients" is more commonly used in both the legal and conveyancing sectors, the term "customers" is used throughout the AML/CFT Act. In this guideline please read the term "customers" as referring to your "clients"
DBG	Designated business group
DIA	Department of Internal Affairs
DNFBP	Designated non-financial business or profession
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
Financing terrorism offence	As defined in section 8(1) of the Terrorism Suppression Act 2002
goAML	FIU reporting portal
Law firm	A barrister or a barrister and solicitor who is practising on the barrister's or a barrister and solicitor's own account in sole practice; or, two or more barrister and solicitors practising law in partnership, (ie, a partnership); or, an incorporated law firm
ML/TF	Money laundering or terrorist financing
Money laundering offence	As defined in section 243 of the Crimes Act 1961
PEP	Politically exposed person
PTR	Prescribed transaction report
Reporting entities	Casinos; designated non-financial businesses or professions; financial institutions; high-value dealers; and the New Zealand Racing Board
SAR	Suspicious activity report
SPR	Suspicious property report
Supervisors	Supervisors have responsibility for monitoring compliance with the AML/CFT Act. DIA is the supervisor for reporting entities in the legal and conveyancing professions among other sectors. The Reserve Bank of New Zealand and the Financial Markets Authority supervise other sectors

Introduction

This guideline is for law firms, conveyancing practitioners and incorporated conveyancing firms who have compliance obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act or the Act) from 1 July 2018.[2] Those that do are "reporting entities" for the purposes of the Act. The Department of Internal Affairs (DIA) is the supervisor for the legal and conveyancing professions.[3]

As your supervisor, DIA expects lawyers[4] and conveyancers to:

1. Know your money laundering and terrorist financing (ML/TF) risks
2. Know if the AML/CFT Act applies to your business
3. Know how legal professional privilege applies
4. Know your compliance requirements
5. Know your customer
6. Know the red flags of ML/TF
7. Know your AML/CFT supervisor
8. Know where to get support

This guideline will help reporting entities in the legal and conveyancing professions to meet each of the expectations identified above. The AML/CFT Act requires that reporting entities have regard to any guidance produced by the AML/CFT supervisor and the Commissioner of Police when developing their risk assessment and AML/CFT programme.[5]

This guideline does not provide a "how to" guide or additional prescription to complement the AML/CFT Act. A one-size-fits-all approach will not work well for most reporting entities. Instead, this guideline will help lawyers and conveyancers increase their awareness of ML/TF risks, and provides prompts for how to manage your compliance.

Over time new case law may become available, new regulations may be made, or existing regulations amended, and this guideline will be updated. The DIA website provides a reference page to find the relevant regulations.[6] DIA will inform reporting entities of any new regulations or updates to existing guidance. The AML/CFT supervisors have already produced a wide range of guidance, much of which lawyers and conveyancers are likely to find useful. The guidelines are all available on the DIA website and are referred to throughout this guideline where relevant.[7] Other guidelines may be produced in the future as needed.

You can contact us at amlphase2@dia.govt.nz if you have further questions.

1. Know your ML/TF risks

Undetected financial crime reduces the integrity of national and international financial systems, distorts the economy and diminishes opportunities for legitimate economic activities. The Government loses tax revenue, while people are rewarded for criminal behaviour. New Zealand is at risk of being targeted by international criminal networks to inject the proceeds of crime into the international financial system. Money laundering and financing of terrorism are not solely international crimes. Domestic criminals use a variety of methods to conceal the proceeds of their criminal activities from authorities in New Zealand.

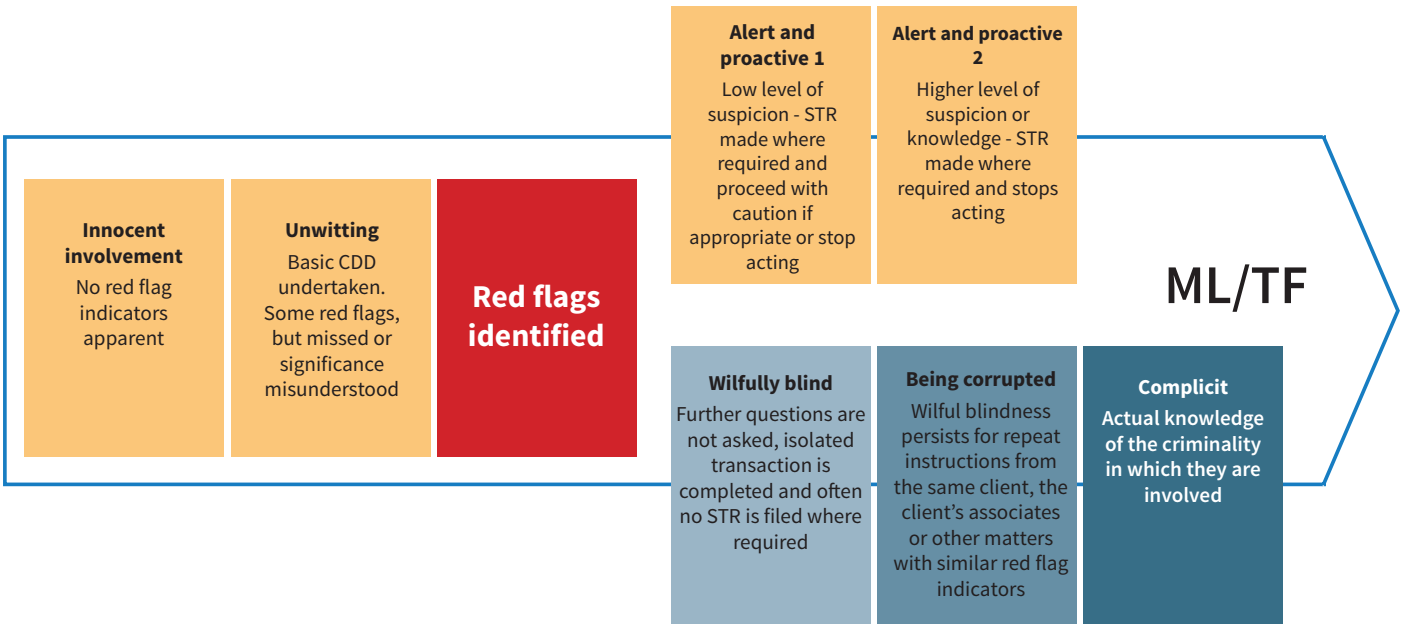
The Financial Action Task Force (FATF) is an inter-governmental body that sets standards for combating ML/TF and other related threats to the integrity of the international financial system. New Zealand has included legal and conveyancing professionals in the AML/CFT system in response to recommendations made by the FATF.[8] The FATF has provided the following diagram to describe the two potential trajectories of legal professionals' involvement in ML/TF.[9]

Using legal professionals is attractive to some people because these professionals are required for the completion of certain kinds of transactions and because their specialist legal or notarial skills can be misused to assist the laundering of criminal proceeds or funding terrorism. Both legal and conveyancing professionals add respectability to transactions.

When these professionals lack ML/TF awareness, they are more at risk of inadvertently helping criminals.

Given these risks, and the FATF recommendations, the Government has chosen to engage gatekeeper professions in the collective efforts to deter and detect these crimes. The more eyes and ears attuned to the indicators (or red flags) of these crime types, the more likely people will struggle to benefit financially from criminal activities. By expanding the AML/CFT system to include the gatekeeper professions, the Government intends that gatekeepers will be better able to protect themselves from customers who launder money and finance terrorism. The AML/CFT system has been designed to help businesses achieve the level of compliance required to assist authorities to identify criminal customers.

Compliance also has a value for business risk management. Professionals closely guard their reputations. It is in their interest to avoid relationships with customers who will cause them disrepute in the legal community or censure by their professional bodies or government authorities. Businesses that fail to comply and are misused by criminals risk negative media coverage both in New Zealand and internationally. This also diminishes New Zealand's international reputation as a safe place to do business.



2. Know if the AML/CFT Act applies to your business

Law firms, conveyancing practitioners and incorporated conveyancing firms will have obligations under the AML/CFT Act when they conduct certain activities (referred to throughout this guidance as "captured activities"). This section provides more detail about these captured activities and why they are included in the Act. The following flow chart provides a quick way to check if you are captured under the AML/CFT Act.

Am I captured by the AML/CFT Act as a DNFBP?

Are you a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, a real estate agent, or a trust and company service provider?

YES

Do you do any of these activities in the ordinary course of business?

Act as a formation agent of legal persons or legal arrangements

OR

Act as, or arrange for a person to act as, a nominee director, nominee shareholder or trustee in relation to legal persons or legal arrangements

OR

Manage client funds (other than sums paid for professional services), accounts, securities or other assets

OR

Provide real estate agent work to effect a transaction

OR

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 by the definition of a DNFBP)

OR

Engage in or give instructions on behalf of a customer 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 customer in relation to creating, operating, and managing a legal person, and any other legal arrangement

YES

You are captured and must comply with the AML/CFT Act

UNLESS

There is an exemption which excludes your business from compliance requirements

NO

You are not captured

NB: If in the future you are asked to conduct any activity described above, you will need to determine if you are captured by the Act

How to know if you are captured by the AML/CFT Act

The AML/CFT Act is activities-based. Lawyers and conveyancers need to develop a thorough understanding of:

- Exclusions to and exemptions from the AML/CFT Act
- What conducting captured activities "in the ordinary course of business" means
- What obligations are related to the captured activities
- How to determine whether advice to a customer is a captured activity
- The nature of each of the activities that are captured by the AML/CFT Act

This section elaborates on the captured activities that lawyers and conveyancers may conduct. The AML/CFT Act imposes obligations only for these captured activities.[10] The obligations of the AML/CFT Act do not apply to any other activities that a lawyer or conveyancer carries out in the ordinary course of business.

Exclusions to and exemptions from the AML/CFT Act

There are a number of ways in which entities, transactions or activities can be exempt from the Act's requirements. For instance, the AML/CFT (Definitions) Regulations 2011[11] provide a number of specific exclusions to the definition of "reporting entity", and the AML/CFT (Exemptions) Regulations 2011[12] provide a range of exemptions for specific classes of transactions and services. There are also Ministerial exemptions, which can exempt (from any or all of the provisions of the Act) either specific reporting entities, or classes of reporting entities, as well as transactions or classes of transactions.[13] The AML/CFT (Class Exemptions) Notice 2014[14] provides further detail about class exemptions.

The Ministry of Justice handles Ministerial exemption applications and provides advice to the appropriate Minister who makes the final decisions. Exemptions may be granted by the Minister subject to sections 157 to 159 of the AML/CFT Act.[15] Please review these sections if you are considering making an application.

Interpreting "ordinary course of business"

Activities must be done in the ordinary course of business to be captured by the Act. The AML/CFT supervisors have issued guidance on how to interpret "ordinary course of business."[16] Whether an activity is in your "ordinary course of business" will always be a matter of judgement depending on the nature of your business. Some relevant factors to take into consideration would be whether the activity:

- Is normal or otherwise unremarkable for your business
- Is frequent
- Is regular (meaning predictable, consistent)
- Involves significant amounts of money
- Is a source of income
- Involves significant resources
- Involves a service offered to customers

It is likely that the activity is in the ordinary course of your business if one or more of these factors apply.

If you are conducting a captured activity in your personal capacity (as opposed to in your professional capacity) you are not captured by the AML/CFT Act. An example of this would be if you are a trustee for a registered charitable trust in your local community in your personal capacity.

If, after considering the AML/CFT Act and this guidance, you are still unsure as to whether you are a reporting entity, you should seek independent legal advice or contact us at amlphase2@dia.govt.nz.

What obligations are related to the captured activities

The AML/CFT Act requires you to know who your customers are (as well as who any beneficial owners of your customer are, and any person acting on behalf of your customer) by conducting customer due diligence (CDD) to the level required before you conduct a captured activity or establish a business relationship.

How to determine whether advice provided to your customer is captured

There will be circumstances where you give advice in relation to a captured activity (without necessarily then carrying out the activity). Generally, advice alone, in the absence of any actual captured activity on the lawyer or conveyancer's part, will not be caught by the definition of "designated non-financial business or profession".

It may be that in practice you expect to provide a mixture of advice and captured activities for a customer over a period of time. In those circumstances, you would need to conduct CDD to the required level *prior* to establishing a business relationship with the customer (and prior to providing any advice).

You also need to be aware of your obligations to report suspicious activities, which can include requests or enquiries about particular services you offer from potential new customers (regardless of whether you ultimately provide those services).

Activities captured by the AML/CFT Act

This section outlines the activities that are captured by the AML/CFT Act and provides some examples of what these activities may look like for lawyers and conveyancers. The examples are indicative and not exhaustive. As we learn from our experiences regulating the legal and conveyancing professions, we will be able to provide more information about supervisor expectations in certain scenarios.

When in doubt about whether you undertake any of the activities described below, please look to the explanations. If you are still uncertain, contact DIA at amlphase2@dia.govt.nz or seek legal advice.

Activity: Acting as a formation agent for legal persons or legal arrangements

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, acts as a formation agent of legal persons or legal arrangements, is captured by the AML/CFT Act as a reporting entity.

The term "legal arrangement" is defined in the AML/CFT Act[17] as meaning a trust, a partnership, a charitable entity (within the meaning of section 4(1) of the Charities Act 2005), and any other prescribed arrangements that involves a risk of ML/TF.[18]

Examples of this kind of activity in practice

- You register a company on behalf of a customer.
- You create a registered charitable trust for a customer.

ML/TF risks associated with this activity

When a lawyer is engaged to register a company or partnership, the actual ownership of the company or partnership being formed can be concealed or obscured – for example, where shell companies, multiple layers of ownership or other complex legal structures are used. Setting up a trust can also be a way to create a perception of distance between assets and their beneficial owners. International evidence shows that using charitable organisations (such as incorporated societies and charitable trusts) is also an identified method that criminals use to launder their money or to finance terrorism. (Please see section 6, case studies 5 and 6 in Appendix A, and the red flags in Appendix B.)

Activity: Acting as, or arranging someone to act as, a nominee director, nominee shareholder or trustee

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, acts as, or arranges for a person to act as, a nominee director, nominee shareholder or trustee in relation to legal persons or legal arrangements, is captured by the AML/CFT Act as a reporting entity.

Examples of this kind of activity in practice

- You act as a nominee director of a company that is registered in New Zealand.
- You act as a trustee for a registered charitable trust in your local community.
- You arrange for a person to act as a nominee shareholder for a company.

ML/TF risks associated with this activity

If a lawyer is acting as a nominee director, nominee shareholder or a trustee for a company or other legal arrangement (such as a trust or charity), others may gain a false impression of legitimacy for the activities undertaken by the company or legal arrangements. This lack of visibility provides criminals with the opportunity to use their companies or other legal arrangements for money laundering or other financial crime without being detected. The possibility of detection is made less likely because they can do this while maintaining the impression of oversight by reputable New Zealand-based directors.

Lawyers who act or arrange for someone to act as a nominee director, nominee shareholder, or trustee need to establish the reason why this arrangement is required. We expect that lawyers establish that there is a legitimate economic purpose of the company or legal arrangement and know who its beneficial owners are. (Please see section 6 and the red flags in Appendix B.)

Activity: Providing an office or address for a company or legal arrangement

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, provides a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal persons or arrangement, is captured by the AML/CFT Act as a reporting entity.

The only exception to this is where the office or address is provided solely as an ancillary service to the provision of other services that are not otherwise captured by definition of "designated non-financial business or profession" in the AML/CFT Act.

Example of this kind of activity in practice

- You have assisted an offshore company to set up a subsidiary in New Zealand and allow the subsidiary to use your address as its registered office address.

ML/TF risks associated with this activity

For a person who is intent on money laundering or committing other financial crime, the use of an address that is not their physical location is attractive. It allows them to keep anonymity and distance from the transactions they are undertaking, and if it is the address of a lawyer, it adds a perception of legitimacy to their activities. It also makes it more difficult for law enforcement to track them down in person.

Activity: Managing client funds, accounts, securities, or other assets

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, manages client funds (other than sums paid as fees for professional services), accounts, securities, or other assets, is captured by the AML/CFT Act as a reporting entity.

DIA's view is that managing payments to or from your customers' accounts is captured; and, with the exception of payments for professional fees, any instance where you receive or hold client funds and deal with those funds in accordance with client instructions will also be captured.

Examples of this kind of activity in practice

- You hold customer funds for a property sale in your trust account until settlement date and then transfer those funds to the vendor.
- You make investments on behalf of customers in securities and/or other assets.
- You manage the sale and/or purchase of trust assets for your customer.
- You disburse the funds received into your trust account from a litigation settlement to your customer.
- You exercise the enduring power of attorney that you hold for a customer who has lost mental capacity by making payments from their personal account to meet their financial obligations.

ML/TF risks associated with this activity

Some people will try to avoid accessing banking services typically used in transactions to obscure the trail of money changing hands as a means to hide their criminal activities. One way to obscure this trail or to add an appearance of legitimacy is to try to use the trust accounts or professional services of legal and conveyancing professionals.

Activity: Providing real estate agency work to effect a transaction

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, provides real estate agency work (within the meaning of the Real Estate Agents Act 2008) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008), is captured by the AML/CFT Act as a reporting entity.

ML/TF risks associated with this activity

Property purchases are a recognised typology for money laundering. These purchases allow for large amounts of criminal proceeds to be stored in an asset that appreciates. Sales and purchases of property can provide the appearance of legitimacy for the acquisition and movement of large sums of money. Residential and commercial properties purchased for money laundering purposes can also be used as bases for other criminal operations – such as clandestine laboratories for the production of illicit drugs.

Activity: Engaging in or giving instructions on behalf of a customer to another person for a range of specified services (as below)

In the definition of "designated non-financial business or profession" a law firm, incorporated conveyancing firm or conveyancing practitioner who, in the ordinary course of business, does any of the activities listed in the next box is captured by the AML/CFT Act as a reporting entity.

The activities specified in the following box apply to situations where lawyers or conveyancers either engage in the following activities themselves, or give instructions on behalf of a customer to another person for those activities. This means that if you are instructing a third party to undertake activities on behalf of your customer, you are captured by the AML/CFT Act – as is the third party you instruct if they fall within the definition of either "designated non-financial business or profession" or "financial institution".[19]

Engaging in or giving instructions on behalf of a customer to another person for –

A. any conveyancing (within the meaning of section 6 of the Lawyers and Conveyancers Act 2006)[20] to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008),[21] namely,—
   - the sale, the purchase, or any other disposal or acquisition of a freehold estate or interest in land:
   - the grant, sale, or purchase or any other disposal or acquisition of a leasehold estate or interest in land (other than a tenancy to which the Residential Tenancies Act 1986 applies):[22]
   - the grant, sale, or purchase or any other disposal or acquisition of a licence that is registrable under the Land Transfer Act 1952:[23]
   - the grant, sale, or purchase or any other disposal or acquisition of an occupation right agreement within the meaning of section 5 of the Retirement Villages Act 2003:[24]

B. a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008);[25] or

C. the transfer of a beneficial interest in land or other real property; or

D. a transaction on behalf of any person in relation to the buying, transferring, or selling of a business or legal person (for example, a company) and any other legal arrangement; or

E. a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement"

You should read both (D) and (E) to mean undertaking any one of the activities mentioned, not a combination of all activities at once.

ML/TF risks associated with this activity
The key risk with all the activities described in the box above is the anonymity and appearance of legitimacy that may be gained by the customer through the lawyer or conveyancing practitioner engaging in the activities, or giving instructions to another person on their behalf for those activities. The person being instructed by the lawyer or conveyancer will be unlikely to have any face-to-face contact with the actual customer. If the customer has criminal intentions, there would be a protective layer of the lawyer or conveyancer and the third person between the customer and the transaction they are instructing. (Please see section 6; case studies 3, 4 and 9 in Appendix A; and the red flags in Appendix B.)

3. Know how legal professional privilege applies

The Act does not require any person (lawyer or otherwise) to disclose any information that the person believes, on reasonable grounds, is a privileged communication.

The AML/CFT Act requires all reporting entities to report suspicious activities by filing suspicious activity reports (SARs) with the Financial Intelligence Unit (FIU). If it is possible for you to file an SAR without disclosing a privileged communication, you must do so. It is accepted that in some cases this will not be possible.

A "privileged communication" is defined in section 42 of the AML/CFT Act as:[26]

- A confidential communication between a lawyer and another lawyer or a lawyer and his or her client made for the purpose of obtaining or giving legal advice or assistance; or
- A communication that is subject to the general law governing legal professional privilege or is specified in sections 53–57 of the Evidence Act 2006[27]

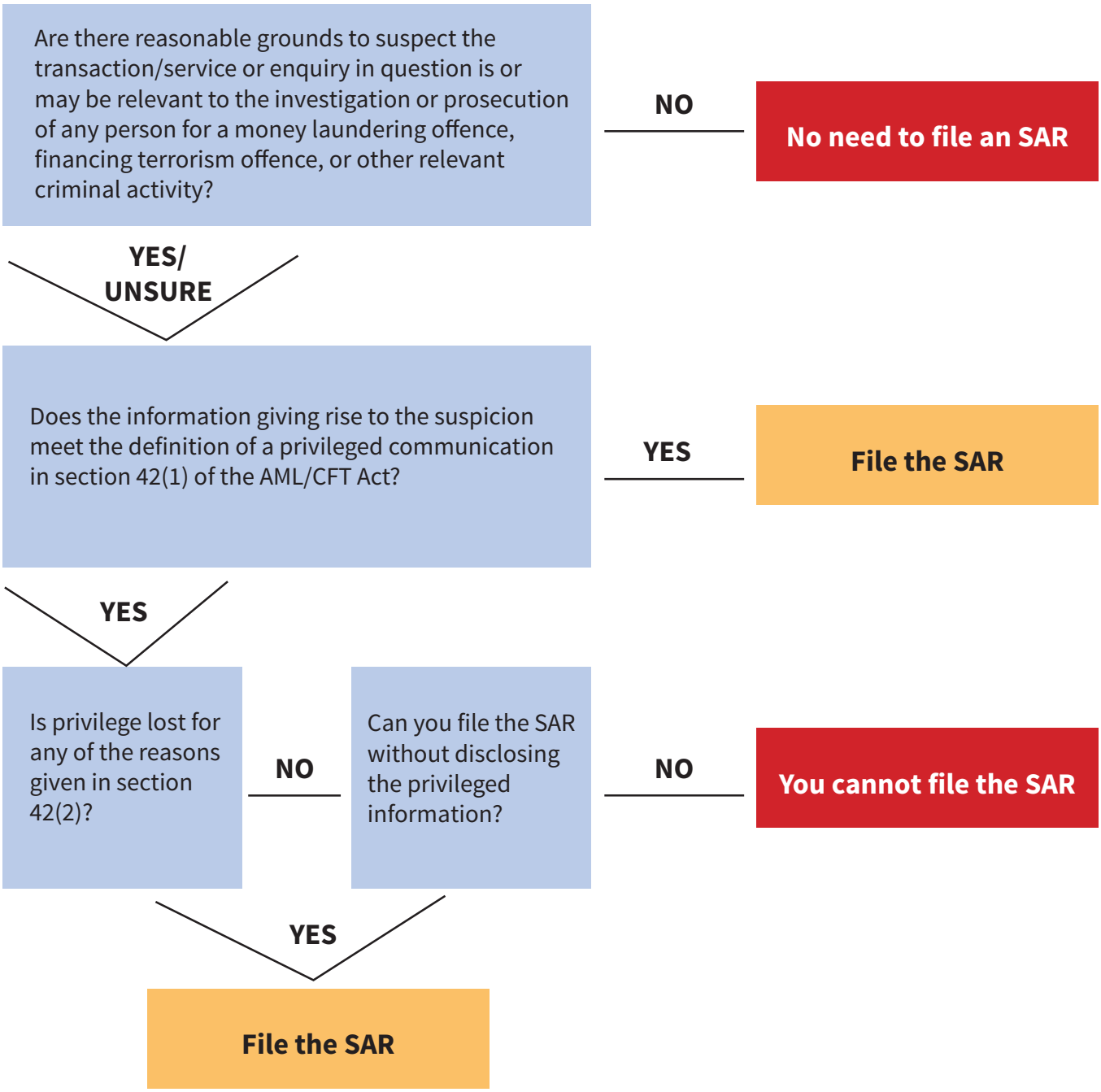
A privileged communication can be oral or written, and it can include any information or opinion. It also includes communications between agents of lawyers and/or agents of customers.

However, the AML/CFT Act provides that a communication is not a privileged communication if:

- There is a prima facie case that it is made/received/compiled or prepared for a dishonest purpose or to enable or aid the commission of an offence; or
- The information consists wholly or partly of (or relates to) receipts, payments, income, expenditure, or financial transactions of any person and is contained in (or comprises the whole or part of) any book, account, statement or other record kept by the lawyer in connection with the lawyer's trust account

It will be for lawyers to determine whether a "prima facie case" exists on the facts before them. This may involve considering whether there is some credible evidence that a communication is made for a dishonest purpose, or to enable the commission of a crime.[28]

Lawyers may find it helpful to ask the following questions when considering whether to file an SAR:



You should keep detailed records of any such assessment.

An SAR must be filed as soon as practicable, and no later than three working days after you become aware of facts that would objectively justify a suspicion (or by reasonable diligence would have become aware of).[29] The failure to do so is an offence (see section 92 of the Act).[30] It is not a defence if a reporting entity did not actually consider a transaction to be suspicious, when objectively it should have. It is a defence if a reporting entity believes on reasonable grounds that the documents or information relating to the activity were privileged communications.

Generally, a person who makes an SAR will be immune from civil, criminal or disciplinary proceedings as a result. This will not be the case if information was disclosed in bad faith, or if the information was disclosed by a lawyer despite the existence of reasonable grounds to believe the information was privileged. This highlights the importance of making a considered assessment in every case.

AML/CFT supervisors and the Commissioner of Police have a range of powers to require the provision of information and documentation for the purpose of ensuring compliance with the AML/CFT Act. These powers cannot be used to compel any person to disclose a privileged communication. Your AML/CFT programme should outline the procedure for determining and recording whether information is a privileged communication.

If a person refuses to disclose information to a supervisor or the Commissioner of Police on the grounds it is a privileged communication, either the person, the Commissioner of Police or the supervisor can apply to a District Court Judge to determine whether or not the claim of professional privilege is valid. This option is not available to a lawyer who is deciding whether a communication is privileged when considering whether to file an SAR.

If a person refuses to disclose information to a supervisor or the Commissioner of Police on the grounds it is a privileged communication, either the person, the Commissioner of Police or the supervisor can apply to a District Court Judge to determine whether or not the claim of professional privilege is valid.[31] This option is not available to a lawyer who is deciding whether a communication is privileged when considering whether to file an SAR.

Where the AML/CFT Act is silent about privilege, the normal principles apply. For example, you will not be able to disclose privileged information to any external auditor without a waiver of privilege from the customer concerned (bearing in mind the customer – not the lawyer – is the holder of privilege).

If you require additional support, you can access more detailed information and advice on professional privilege from the New Zealand Law Society.

4. Know your compliance requirements

Any law firm, conveyancing practitioner or incorporated conveyancing firm, either existing or established after the introduction of the AML/CFT Act, that conducts captured activities will be a reporting entity and will have to comply with the Act. You will not be excused from compliance on the basis that to comply would breach any contract or agreement.[32]

Compliance requirements for reporting entities

Appoint a compliance officer – Section 56
Reporting entitles must appoint a compliance officer who will have responsibility for administering and maintaining the AML/CFT Programme. An employee should be appointed to this role who reports to a senior manager. In the case of a sole practitioner, we would expect the sole practitioner to be the compliance officer. If that is not possible, an external person must be appointed as a compliance officer.

Conduct a risk assessment – Section 58
Reporting entities are required to undertake an assessment of the risks posed to their business by money laundering and financing of terrorism crimes. The risk assessment should be in writing and be informed by the *Phase 2 Sector Risk Assessment*, which is available on the DIA website.

Develop an AML/CFT programme – Section 57
The AML/CFT programme must be based on the risk assessment described above and be in writing. It should include procedures, policies and controls for ensuring all compliance obligations are adequately and effectively met.

Maintain your compliance programme

Conduct customer due diligence (CDD) – Part 2, Subpart 1
Reporting entities must conduct CDD when conducting an occasional transaction or activity or when establishing a business relationship with a client who is requesting assistance with a captured activity, or when an existing client makes this kind of request (if the reporting entity doesn't hold all the information required already). There are three levels of CDD depending on the circumstances.

Keep records – Sections 49–55
Reporting entities must keep records of transactions, suspicious activities, the documents verifying the identities of customers and other parties or beneficiaries, and any other related records that may be of interest to the supervisor. Records must be kept at least five years.

Ongoing customer due diligence and ongoing account monitoring – Section 31
Reporting entities are required to undertake ongoing CDD and ongoing account monitoring. This is to ensure that you have ongoing confidence that the business relationship and the transactions within the relationship are consistent with the customer's business and risk profile, and you can spot any suspicious activity early.

Review your compliance programme – Section 59
The supervisor expects reporting entities to conduct a regular review of their compliance programme. This is to ensure that any business changes or new risks in the operating environment are referenced in the programme and it remains fit-for-purpose.

Report and audit

Submit an annual report – Section 60
Reporting entities must submit an annual report. This report must be in the prescribed form and be submitted to the supervisor at the time set by the supervisor. The report must take into account the results and implications of the audit and any information prescribed in the regulations.

Audit your risk assessment and compliance programme every two years – Section 59A
At least every two years a reporting entity must review its risk assessment and compliance programme and have it audited by an independent person who is suitably qualified to conduct the audit. Supervisors may also require an audit to be undertaken on request at shorter notice.

Report to the FIU

Report to the Financial Intelligence Unit – Subparts 2 and 2A
When reporting entities identify suspicious activity, they must report it to the FIU. They should also submit prescribed transaction reports to the FIU as necessary. Lawyers will not be required to submit any privileged communication (as defined in the Act) in either report category.

Compliance requirements

This section provides guidance on:

- The risk-based approach that reporting entities need to take when developing their AML/CFT programme
- The range of procedures, policies and controls reporting entities must include in their AML/CFT programme to comply with the AML/CFT Act
- Things to consider if you wish to establish a designated business group to share some aspects of your AML/CFT programme and its implementation

Section 5 provides more thorough detail about compliance requirements for CDD. Information on where to access other support to comply is noted in section 8.

Risk-based compliance

The AML/CFT regulatory system in New Zealand is "risk-based". This means each reporting entity must assess the risk its own business faces from money launderers and terrorist financers. You must then apply suitable procedures, policies and controls to effectively manage the risks you have identified. Compliance resources can then be targeted primarily at high-risk areas, which should reduce the overall compliance cost for your business.

You are the best judge of the risks your business is exposed to and how you can most effectively mitigate those risks in line with the requirements of the AML/CFT Act. As your supervisor, DIA expects you to genuinely and accurately assess the ML/TF risks to your business and then apply a suitable and proportionate AML/CFT programme.

AML/CFT programme – procedures, policies and controls

AML/CFT compliance cannot be achieved with a "set and forget" approach. The AML/CFT programme needs to be fully implemented within the business. It should be a living and adaptable programme. Your specific compliance obligations under the AML/CFT Act are summarised as follows.

Appoint a compliance officer

You must appoint an AML/CFT compliance officer to administer and maintain your compliance programme.[33] The compliance officer should be an employee of the business who reports to a senior manager or partner of the business. If practising on their own account, a lawyer or conveyancer would be expected to act as the compliance officer themselves and take full responsibility for all compliance requirements unless there is a reason why they cannot. In that case they should appoint a third party to take on this duty.[34]

When you have appointed your compliance officer, or if your compliance officer or other contact information changes, it is important that you advise us at amlphase2@dia.govt.nz. This enables us to communicate effectively with you and provide you with important information and updates.

Conduct a risk assessment

Your first step to compliance should be to conduct a risk assessment. All reporting entities must undertake a risk assessment, and it must be in writing. The specific requirements for a risk assessment are set out in section 58 of the AML/CFT Act.[35] The supervisors have provided guidance on how to conduct a risk assessment.[36] The AML/CFT Act requires that you have regard to guidance produced by the AML/CFT supervisors when developing your risk assessment.[37]

DIA has published its own assessment of the ML/TF risks in the sectors it is responsible for supervising, including in the legal and conveyancing professions.[38] DIA has also developed the *AML/CFT Risk Assessment and Programme: Prompts and Notes* (Prompts and Notes) guideline, which outlines the factors to be considered in a risk assessment along with some prompts for things to think about when completing a risk assessment and developing your AML/CFT programme.[39] It provides prompts to help businesses undertake their risk assessment in a way that reflects both the size of their business and their level of risk. In addition, the Financial Markets Authority has published a step-by-step guide for drafting a risk assessment.[40] Together, these resources will help businesses to conduct a realistic assessment of their ML/TF risks so that their AML/CFT programmes can be proportionate to the risks assessed.

You must review and update your risk assessment when there is any material change to the business, its service offerings, or its customer base, or when deficiencies in the effectiveness of the risk assessment are identified. As methods and techniques (known as "typologies") of ML/TF adapt and change, the nature of the risks posed to a business may change also. It is important that lawyers and conveyancers keep up-to-date with relevant changes in typologies. The Quarterly Typology Reports published by the FIU are a good source of typology information.[41]

Set up an AML/CFT programme

Once a risk assessment has been conducted, all reporting entities must develop an AML/CFT programme that includes internal procedures, policies and controls to detect and manage the risk of ML/TF.[42] The AML/CFT Act requires that you have regard to guidance produced by the supervisor when developing your AML/CFT programme.[43] The supervisors' guidance on developing an AML/CFT programme is available on the DIA website.[44]

The supervisors' guidance is generic in nature. It does not provide prescriptive instructions on how businesses can ensure they are compliant with the AML/CFT Act. This is because each business has unique circumstances that determine their exposure to ML/TF risks, which need to be understood and factored into their unique AML/CFT programme. Businesses will need to apply their own judgement, and where there are questions about compliance they can either ask the supervisor for general information, or seek independent legal advice.

Customer due diligence

Section 5 in this guideline is dedicated to explaining your CDD obligations.[45]

Record keeping

You must keep adequate records as outlined in sections 49 to 55 of the AML/CFT Act. This will enable you to operate your AML/CFT programme effectively and enable it to be audited by an independent auditor and reviewed by the supervisor on request. Records must either be kept in written form in English or be readily accessible and readily convertible into written form in English.

You must keep your records for at least five years. The supervisor or the Commissioner of Police may ask you to keep records for longer in some circumstances. After five years, the records can be destroyed unless there is a lawful reason why they should be retained – for example, the need to comply with another enactment or to enable you to carry on your business.

You must keep the following records:

Record type	Retention period
Transaction records sufficient to enable the transactions to be fully reconstructed at any time[46]	5 years from the completion of the transaction
Any reports of suspicious activities[47]	5 years after the report is made
Identity and verification evidence (as reasonably necessary to enable the nature of the evidence to be readily identified at any time)[48]	5 years from the end of the business relationship or the completion of the occasional transaction or activity
Risk assessments, AML/CFT programmes and audits	5 years after the date on which they cease to be used on a regular basis
Information relevant to the establishment of a business relationship and any other records that explain the nature and purpose of a business relationship and the activities relating to that business relationship[49]	5 years from the end of the business relationship

You are also strongly advised to keep any detailed records of your assessment of whether an SAR is required, including any determinations of whether information is legally privileged.

Ongoing customer due diligence and ongoing account monitoring

When you have established a business relationship, you must conduct ongoing CDD and undertake ongoing account monitoring.[50] For more information, please see “Ongoing CDD and account monitoring” on page 39.

Review your AML/CFT programme

You must regularly review your risk assessment and AML/CFT programme to ensure it remains up-to-date and to identify and remedy any deficiencies.[51] Your records should show evidence of updates that address any identified deficiencies in its effectiveness. Ways to do this would be to keep a record of version history or retain evidence demonstrating reviews and updates.

Annual reporting to your supervisor

Like all reporting entities, you are required to submit an annual report each year covering the period July to June.[52] The date for submission is advised by the supervisor each year, and you will usually have two months to submit. This means the first annual report will be due approximately at the end of August 2019. A new annual report template has been designed for lawyers, conveyancers, accountants and real estate agents and is provided for by regulations.[53] Please go to the DIA website for more information.[54] All reporting entities are also expected to respond to any requests for subsequent information from the supervisor in a timely manner.

Independent audits of your risk assessment and AML/CFT programme

Every two years, you are required to have an independent audit of your risk assessment and AML/CFT programme.[55] An independent audit aims to ensure that documents remain up-to-date, that any deficiencies in programme effectiveness are identified, and that any necessary changes can be made. For guidance, please see the *Guideline for Audits of Risk Assessments and AML/CFT Programmes*, which is available on the DIA website.[56]

The AML/CFT Act requires you to appoint someone who is independent and suitably qualified to conduct the audit.[57] The audit cannot be undertaken by someone from within the business unless a sufficient degree of independence can be demonstrated. For instance, a very large firm with a dedicated audit function would likely be able to show a sufficient degree of independence. Someone who has been involved in the establishment of the compliance programme (such as completing the risk assessment and/or writing the AML/CFT programme) cannot conduct the audit.[58] The auditor does not need to be a chartered accountant or qualified to undertake financial audits.

To be suitably qualified we expect that your auditor would have a working knowledge of the AML/CFT Act and its complexities.

A copy of the independent audit must be provided to the supervisor on request. The supervisor can instruct a reporting entity to have a new independent audit undertaken at any time.

Reporting to the FIU

As a key part of your AML/CFT obligations, in specific circumstances you need to report certain information to the FIU. Each reporting entity will have visibility over different parts of any one chain of events leading to a transaction or following on from a transaction. Each type of report will provide the FIU with one set of information, complementing other types of reports providing further information. It may be that the report you provide will be the one crucial piece that brings enough of the puzzle together to lead the FIU to take appropriate action against a criminal.

When you need to report

From 1 July 2018, you will be required to submit suspicious activity reports[59] (SARs) and prescribed transaction reports (PTRs). From that date you will no longer be required to submit reports under the Financial Transactions Reporting Act 1996.

Suspicious activity reports

Section 39A of the AML/CFT Act defines a "suspicious activity", and section 40 of the Act requires a reporting entity to report a suspicious activity to the FIU as soon as practicable, but no later than three working days after forming its suspicion. This has been held to mean that a reporting entity must report a suspicious activity within three days of the point at which the reporting entity becomes aware of facts that would objectively justify a suspicion (or by reasonable diligence would have become aware of them).[60] It is not a defence that a reporting entity did not actually consider an activity to be suspicious in circumstances where it objectively should have. For further detail on making an assessment as to whether to file an SAR, please see section 3.

Prescribed transaction reports
A prescribed transaction is an international wire transfer of NZD $1,000 or more conducted through a reporting entity or a domestic physical cash transaction of a value equal to or above NZD $10,000.[61] Please refer to page 37 for more detail on wire transfers (including international wire transfers).

Only an ordering institution and a beneficiary institution are required to file a PTR in respect of an international wire transfer.

An "ordering institution" is defined as "any person who has been instructed by a payer to electronically transfer funds controlled by the payer to a payee via a "beneficiary institution". The ordering institution will be the first reporting entity to transfer the funds that are the subject of the international wire transfer – for instance, a law firm that holds customer funds in a trust account, and transfers those funds (including via the formal banking system) to an overseas beneficiary bank.

A reporting entity that simply passes on an instruction to transfer funds, without actually transacting, will not be required to file a PTR. A "beneficiary institution" (in relation to a wire transfer from an ordering institution) is defined as "any person who receives those funds and then makes those funds available to a person (the payee) by crediting it to an account held by the payee or paying it to the payee". The beneficiary institution will be the last reporting entity in the chain that receives the funds before making them available to its customer (the beneficiary of the transaction).

Usually the bank will be a beneficiary institution; however, in some cases the beneficiary institution may be a different reporting entity, such as a law firm, depending on where the funds (intended for the customer) end up.

PTRs are intended to add further transparency to the financial system by making the range of methods of ML/TF even more difficult to hide. PTRs will also improve the detection and disruption of organised crime.

Suspicious property reports
You also need to be aware of your obligations to submit "suspicious property reports" (SPRs) under the Terrorism Suppression Act 2002. If you are in control of property that you suspect (on reasonable grounds) is property that is owned or controlled, directly or indirectly by a "designated terrorist entity" (or property derived or generated from that type of property), you must report that suspicion in accordance with sections 43 and 44 of the Terrorism Suppression Act (note that, like the AML/CFT Act, the Terrorism Suppression Act protects privileged communications).[62] The SPR must be submitted as soon as practicable after forming your suspicion. Designated terrorist entities are identified on a publicly available list that is updated by the New Zealand Police.[63] If you find a match on a list other than New Zealand's terrorist designation list, the reporting entity is required to submit an SAR to the FIU.

How to report
The FIU has issued guidance on how to submit reports using their goAML web-based reporting tool.[64] You must use the specific reporting format provided by the FIU. If you have reported on your customer, you must not disclose this information to your customer or to any person that is not entitled to receive this information.[65] If, after making a report, you are unsure if you need to end your existing relationship with your customer, you may wish to review the respective Conduct and Client Care Rules for lawyers and for conveyancers,[66] or consult the New Zealand Law Society, or seek independent advice. For further discussion on ending or declining business relationships, please see "What to do if you cannot complete CDD" on page 40.

Establishing a designated business group

In certain circumstances, law firms, conveyancing practitioners or conveyancing firms may be able to form a designated business group (DBG) with other entities (whether or not those entities are other law firms or conveyancers or even reporting entities). The term "designated business group" is defined in full in the AML/CFT Act and regulations.[67] In summary, it means a group of two or more persons who have elected (in writing) to form a group to enable some obligations under the AML/CFT Act to be met on a shared basis while the election is in force.

A member of a DBG can rely on another member to carry out certain obligations on their behalf, including CDD (in certain situations).[68] Members can also rely on specified parts of another member's AML/CFT programme, and another member's risk assessment (if relevant), as well as reporting to the FIU. Members may share information and rely on each other, but they still retain responsibility for their own compliance. Any decision to apply to become a DBG should include a thorough consideration of the risks and implications for all members.

The supervisor will consider all applications for DBGs. If you are not sure whether or not your proposed DBG meets the criteria in the definition in section 5(1) of the Act, you are welcome to contact us to discuss. We would prefer if reporting entities test their proposals with us rather than assume they could not apply. If you are interested in applying to form a DBG, we recommend you familiarise yourself with the two available guidelines to assist reporting entities to create DBGs, one on Scope and one on Formation, before you submit an application.[69] The application form is included in the Formation guideline.

5. Know your customer

This section provides information about:

- What a business relationship means and when it starts
- Who to conduct CDD on
- What the different levels of CDD are
- How to use the Amended Identity Verification Code of Practice
- When you can rely on others for CDD
- When to conduct CDD
- What to think about when participating in international transactions
- What to do if you cannot complete CDD

The requirements described in this section are contained in Part 2, subpart 1 of the AML/CFT Act.[70] The supervisors have prepared a range of guidelines that are likely to assist lawyers and conveyancers with undertaking CDD. The guidelines are available on the DIA website.[71]

When a business relationship starts

A business relationship is defined in section 5(1) of the Act as "a business, professional, or commercial relationship between a reporting entity and a customer that has an element of duration or that is expected by the reporting entity, at the time when contact is established, to have an element of duration". This has been held to capture situations where a reporting entity has, or expects to have, a relationship with a customer involving more than one interaction or the carrying out of multiple transactions.[72]

You will need to use your judgement to determine when a business relationship with a customer starts. This is likely to be after initial enquiries have been made, but before any work has commenced.

In the case of a property sale, the business relationship or occasional activity is assumed to have commenced at the point where the customer has engaged the lawyer or conveyancer to undertake the necessary work.

Who to conduct customer due diligence on

You must conduct CDD on:

- Your customer
- Any beneficial owner of a customer
- Any person acting on behalf of a customer

New customers

You may not have to conduct CDD on every new customer. You need to establish at the outset whether they are going to require you to conduct any activity captured by the AML/CFT Act. If they are, you will need to conduct CDD in line with the level of risk you anticipate and in accordance with the requirements in the Act. See further on in this section for the levels of CDD and further explanation of the compliance requirements. If your customer does not require you to conduct a captured activity initially, but over time you are instructed to carry out captured activities, you must ensure you have completed the necessary CDD before you carry out those captured activities.

Existing customers

The term "existing customer" is defined in the Act as a person who was in a business relationship with a reporting entity immediately before the Act began applying to the reporting entity.[73] You must conduct CDD on existing customers if there has been a material change in the nature or purpose of the business relationship with that customer, and you have insufficient information about that customer. When considering what information would be sufficient, you will need to assess the level of risk involved, and whether you hold the necessary identity information, verified to the appropriate level. You should not conduct any captured activity until these requirements are met.

Occasional customers

"Occasional activity" and "occasional transaction" are both defined in the Act.[74] The term "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.

The other people you must conduct CDD on

You must also complete CDD on:	For example:
Any beneficial owner[75] of a customer	Someone who owns more than 25% of a company that is your customer[76]
Any person acting on behalf of a customer	• A person exercising power of attorney for your customer • A legal guardian acting on behalf of a minor who is your customer • An employee of a company that is your customer

You need to have a good understanding of who your customers are and their circumstances and intentions. If you understand the sources of your customer's income and wealth and who else has an interest in their activities – ie, who else benefits – you can make a reasonable assessment about whether your customer's requests are typical, legitimate or potentially suspicious.

The DIA website provides a range of guidelines to help you conduct the appropriate level of CDD on different kinds of customers. There are fact sheets that cover the following CDD topics:[77]

- Acting on behalf of others
- Clubs and societies
- Companies
- Co-operatives
- Sole traders and partnerships
- Trusts

The supervisors have also provided specific guidance on beneficial ownership.[78] Customers that are individuals may be treated as the beneficial owner so long as you believe on reasonable grounds that the person is not acting on behalf of anyone else.[79]

The AML/CFT Act treats trusts as being capable of being customers in their own right, despite a trust not ordinarily having a legal personality. The supervisors have provided a fact sheet to help reporting entities who engage with trusts as customers.[80]

Different levels of CDD

There are three levels of CDD. You will need to be sure you use the right level, which will depend on the unique factors of each business relationship, the characteristics of the customer(s), the nature of the activities and transactions you are facilitating, and the potential for ML/TF risk. The three levels are:

- **Standard CDD** – for most common situations
- **Simplified CDD** – for use with specific customers or customer types that are considered to be low risk for ML/TF – these customers are specified in section 18(2) of the AML/CFT Act[81]
- **Enhanced CDD** – for use when there are factors creating a higher level of ML/TF risk or are otherwise specified in the AML/CFT Act

You must use your own risk assessment and AML/CFT programme to establish the level of ML/TF risk. This will help you determine which kind of CDD to conduct before establishing the business relationship or conducting an occasional transaction or activity.

How to use the Amended Identity Verification Code of Practice

Identity verification needs to be done by collecting and sighting documents, data, or information provided from a reliable and independent source. You are required to keep records of this information.

The Amended Identity Verification Code of Practice provides suggested best practice for anyone conducting name and date of birth identity verification on customers (who are natural persons) that have been assessed to be low to medium risk.[82] The Amended Identity Verification Code of Practice should be read in tandem with the Explanatory Note.[83]

Standard CDD

Lawyers and conveyancers must conduct standard CDD[84] if:

- They establish a business relationship with a new customer
- A customer seeks to conduct an occasional transaction or activity through the law firm, conveyancer or conveyancing practice; or
- In relation to an existing customer, and according to the level of risk involved, there has been a material change in the business relationship and there is insufficient information held about the customer (for example, they are a litigation customer you have dealt with prior to the Act taking effect who is now seeking legal assistance for establishing and managing a business enterprise)

Identity requirements

When standard CDD applies, the following identity information must be gathered about a customer, the beneficial owner(s), and a person acting on behalf of a customer:[85]

- Full name
- Date of birth
- If the person is not the customer, the person's relationship to the customer
- Address or registered office
- Company identifier or registration number
- You must also obtain information about the nature and purpose of the proposed business relationship with the customer, and sufficient information to determine whether enhanced CDD needs to be conducted on the customer[86]

Verification requirements

Lawyers and conveyancers are required to take reasonable steps to ensure that the information gathered is correct. According to the level of risk involved, you need to take reasonable steps to verify the identity of any beneficial owners, and to verify the identity and authority of any person who is seeking to act on behalf of your customer. The supervisors have published a *Beneficial Ownership Guideline* to help you.[87] Verification must be undertaken before the business relationship is established or before the occasional transaction or activity is conducted. There is an exception to this, which is described in "When to conduct CDD" on page 38.

The Amended Identity Verification Code of Practice allows lawyers (among other identified groups) to act as "trusted referees" to verify identity information. It is important to note that lawyers can only do this where they are not themselves party to the activity or transaction with the customer for whom the CDD is being conducted.

Example in practice – setting up a company

A new customer, Mr Kemal Dilan, approaches your law firm seeking assistance to set up a company that would operate as a social enterprise. The company would import sports gear to sell at very low cost to schools and sports clubs in underprivileged suburbs. Mr Dilan would also like you to be involved on an ongoing basis by providing a correspondence address for the company and ongoing advice on request. Your customer is an individual so cannot be on the list of entities where simplified CDD would apply. As you will be required to undertake captured activities for Mr Dilan, your CDD needs to be completed before you undertake any work for the customer. This includes asking a series of questions about the nature and purpose of the company and the people involved, which leads you to determine that there is no need for enhanced CDD.

Steps to complete standard CDD	How this applies to the example
Obtain identity information for all relevant persons and establish the nature and purpose of the intended business relationship.	Mr Dilan states he will be the sole director, shareholder and manager of the business. He provides you with the original of his current passport.
Obtain information about the nature and purpose of the proposed business relationship.	Mr Dilan explains his intention to establish the social enterprise as a way of giving back to his local community and to reduce barriers for children's participation sports activities.
Make a determination of the level of ML/TF risk involved.	After you establish there are no other people with a beneficial interest in the formation of the company (for instance, proposed shareholders) you assess the risk as low.
According to that level of risk, verify the identity of relevant persons, including natural persons using the Amended Identity Verification Code of Practice.[88]	You view and take a clear copy of the passport. You record the date on which you sighted the passport and made the copy.
If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You provide advice to Mr Dilan about the best way to set up his company and register the company for him.

Simplified customer due diligence

You may complete simplified CDD if your customer is one of those listed in the AML/CFT Act. The list includes a range of organisations, including:

- Government departments
- Local authorities
- The New Zealand Police
- State-owned enterprises
- Crown entities
- Registered banks
- Licensed insurers
- Publicly listed companies

For the full list, please see section 18(2) of the AML/CFT Act.[89]

Identity requirements

When simplified CDD applies, you need to record the full name of the entity in question and a brief explanation of how it falls within section 18(2) of the AML/CFT Act.

The following information needs to be gathered about the identity of a person acting on behalf of one of the entities listed in section 18(2) (eg, an employee of one of those organisations):

- Full name
- Date of birth
- The person's relationship to the customer

You also need to obtain information about the nature and purpose of the proposed business relationship between you and the customer.[90]

Verification requirements

You must verify the identity of a person acting on behalf of a customer, and verify that person's authority to act so that you are satisfied you know who the person acting is and that they have the authority to act. Reasonable steps must be taken according to the level of risk involved. This verification must be undertaken before the business relationship is established (or before the occasional transaction or activity is conducted), or before the person acts on behalf of the customer. There is an exception to this timing requirement – see "When to conduct CDD" on page 38.

Example in practice – forming and administering a scholarship fund

You are approached by Ms Sam Vacari, an employee of a local authority, to help with forming a scholarship fund for students who have been accepted to study law at university. The fund seed money will come directly from the local authority's Education Sub-committee budget. You would be engaged to form the scholarship fund as a legal entity and assist with its administration. You have not dealt with Ms Vacari before and you expect that you will be entering a business relationship of some duration with the local authority. The local authority is your customer and is listed in section 18(2) of the Act, so simplified CDD applies. You should assume for the purposes of this example that all other relevant legal obligations have been met.

Steps to complete simplified CDD	How this applies to the example
Identify whether your customer meets the criteria for simplified CDD.	You identify and record that the local authority meets the criteria for simplified CDD.
Obtain information about the nature and purpose of the proposed business relationship.	Ms Vacari explains the intention of the Education sub-committee to support students from the community to study law as this has been identified as a local skills shortage.
Identify all relevant persons that need to be identified.	As the local authority meets criteria for simplified CDD, you only need to obtain information about the identity of the person acting on its behalf, Ms Vacari, as well as her authority to do so – in this case she shows you her New Zealand driver licence and credit card from a New Zealand registered bank with her name on it, and she also shows you a letter from the chair of the local authority's Education Sub-committee outlining her role in establishing the scholarship fund.
Make a determination of the level of ML/TF risk involved.	You determine that the risk is low, so you continue with applying simplified CDD.
According to that level of risk, verify the identity of Ms Vacari and her authority to act on behalf of the local authority using the Amended Identity Verification Code of Practice (IVCOP).[91]	To meet the requirements of the IVCOP, you sight Ms Vacari's drivers licence and credit card, and note her work email address is consistent with her working for the local authority. You decide that given the low risk you do not need to take any further action to verify her identity or the letter that shows she has authority to act on behalf of the local authority. You record this.
If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You then proceed with forming the legal entity which would operate the scholarship fund.

Enhanced CDD

You must conduct enhanced CDD in specific circumstances:

1. If you are establishing a business relationship with, or looking to conduct an occasional transaction or activity for, a customer that is:
   - A trust or another vehicle for holding personal assets
   - A non-New Zealand resident who is from a country that has insufficient AML/CFT systems and measures in place;[92] or
   - A company with nominee shareholders or shares in bearer form
2. If a customer seeks your assistance to conduct a complex or unusually large transaction or an unusual pattern of transactions that have no apparent or visible economic or lawful purpose[93]
3. When you consider that the level of ML/TF risk involved means that enhanced CDD would be required
4. When you have had cause to submit an SAR to the FIU
5. When you determine that your customer is a politically exposed person
6. If you are an ordering institution, an intermediary institution, or a beneficiary institution in relation to a wire transfer; or
7. If you are undertaking an activity that involves the use of new and developing technologies that may favour anonymity

When conducting enhanced CDD you must obtain information about your customer's source of wealth or source of funds.[94] You must record this information and take reasonable steps, according to the level of risk involved, to verify this information using other reliable and independent sources.[95] Where you identify that the origin of your customer's funds or wealth has come from their beneficial owner(s), it may be necessary, according to the level of risk involved, for you to extend your level of verification to include the source of wealth or source of funds of these persons.

You will not need to obtain and verify source of wealth or source of funds for every beneficial owner where they have nothing to do with your customer's source of wealth or source of funds.

The supervisors have published guidance for all reporting entities on enhanced CDD.[96] The following examples have been tailored to suit lawyers and conveyancers. You should assume for the purposes of these examples that all other relevant legal obligations have been met.

Example in practice: Charitable trust entering into a property development

You are approached by a charitable trust that is looking to engage in a large-scale property development for affordable housing units on the outskirts of Christchurch. The property development is being funded with the assets of the trust and promised donations from other charitable organisations and the regional council. The charitable trust will on-sell each of the housing units at cost price to eligible applicants who meet a household income threshold. You are asked to help with conveyancing the land purchase (captured by the AML/CFT Act) and then to help with gaining all the required building consents (not captured).

Steps to complete enhanced CDD	How this applies to the example
Identify which criteria your customer meets to decide the level of CDD you must do.	You must complete enhanced CDD prior to establishing the business relationship because your customer is a trust.
Obtain information about the nature and purpose of the proposed business relationship.	The representative of the charitable trust advises you that the purpose of the property development is to enable low income families to purchase a home.
Determine the initial level of ML/TF risk.	You research the trust's history and determine that the trust has been in existence for a long time and has conducted large-scale charitable projects in the past. You identify that the charitable trust is registered under the Charities Act 2005 and listed on the Charities Register. You review the information on the Charities Register and identify that this is consistent with its involvement in the proposed property development. Your initial determination is that the ML/TF risk is medium.
Identify all relevant persons that need to be identified and gather information about the source of wealth/ source of funds.	You ask the representative of the charitable trust for proof of their identity. You identify that they are listed on the Charities Register as one of the trustees, along with two other persons. You ask to see the trust deed, copy this document and record the full name of the trust, its address and a description of the objects of the trust. You ask to see account documentation from their bank showing incoming donations and other income and outgoings of the charitable trust for a period of time you suggest. You also obtain documents showing the promised donations to the project from other charitable organisations, local businesses and the regional council.

Verify the information gathered, including using the Amended Identity Verification Code of Practice for the identity of individuals[97] (as risk is not deemed to be high).	You ask the trustee you are dealing with to show you his passport. You take a copy of this passport and record the date that you viewed the original. You retain the copy of the trustee's passport on your file. You advise the trustee that you are dealing with that you need to verify the identity of the other two trustees. One of them is based close by and you arrange for her to come and see you with a copy of her passport. You take a copy of this passport and record the date you viewed the original. The third trustee resides in a different town. You therefore request that a lawyer in that town, who is not involved with the charitable trust or their intended activities, certify a copy of the third trustee's passport. You arrange for the certified copy of this passport to be provided to you. To verify the charitable trust's address, you check the Charities Register online. You record that the stated address on the trust deed matches the address on the Charities Register. You review all the documents provided as proof of source of wealth/funds and determine them to be issued by reliable and independent sources (ie known organisations and the regional council). You therefore decide that no further third-party verification of source of funds/wealth is required.
If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You assist with the purchase of land for the property development.

Example in practice: Winding up a family trust

Mr Ralph Swanson and Mrs Marjorie Swanson ask for your help to wind up their family trust in accordance with the trust deed. The Swanson family trust holds a commercial apple export business, an apple orchard, a packhouse, a residential home, five vehicles and other commercial machinery. Mr and Mrs Swanson have run the apple business but are now looking to retire. None of the beneficiaries (Mr and Mrs Swanson's five children) wish to take over the business. Mr and Mrs Swanson are the trustees of the family trust and decide to sell the apple business as a going concern on the open market. The sale will include the orchard, packhouse, the house and vehicles, and the commercial machinery (ie all the trust assets). The proceeds of the sale will be distributed in line with the trust deed.

Steps to complete enhanced CDD	How this applies to the example
Identify which criteria your customer meets to decide the level of CDD you must do.	You complete enhanced CDD because your customer is a trust.
Obtain information about the nature and purpose of the proposed business relationship.	Mr and Mrs Swanson outline their intentions to retire from the apple business and their need for the proceeds of the sale of trust assets to fund their retirement plans and to financially benefit their children who are beneficiaries named in the trust deed.
Determine the initial level of ML/TF risk.	You ask Mr and Mrs Swanson to provide a copy of the trust deed. You note that the trust was established many years ago by a previous local law firm that you had dealings with in the past and knew to be reputable. You determine that the beneficiaries of the trust are all immediate family members. Your initial determination is that the ML/TF risk is low.
Identify all relevant persons that need to be identified and gather information about the source of wealth/source of funds.	You ask to see the trust deed, and you copy this document and record the full name of the trust, its address and the names and dates of birth of the beneficiaries. You gather identity information for the two trustees (Mr and Mrs Swanson) and the beneficiaries (the five children). You check the trust deed and determine that there are no other beneficial owners. You also obtain documentation, such as bank records and accounts audited by an accountant to prove that the assets of the trust have been purchased from legitimate sources. In this case the source is the profits of the apple enterprise which have fully paid off a business mortgage.

Verify the information gathered, including using the Amended Identity Verification Code of Practice for the identity of individuals (as risk is not deemed to be high).	You ask Mr and Mrs Swanson to show you their passports so that you can verify their identities. Mrs Swanson is able to do this; however, Mr Swanson states that he does not have a passport. You ascertain that he does have a New Zealand driver licence and a credit card from a New Zealand registered bank with his name on it. You take copies of these documents and record the dates that you viewed the originals. You retain copies on your file. You ascertain that four of the Swanson children live locally. You arrange for all of them to bring their passports and undertake the same process. You note that the biographical information on the passports matches the information on the trust documents. You find out that the fifth Swanson child currently lives in Scotland. You therefore request that a lawyer in Edinburgh, who has no connection to the fifth Swanson child or the Swanson Family Trust, certify a copy of his passport. You arrange for the certified copy of this passport to be provided to you. When it arrives, you note that the biographical information on the passport matches the information on the trust documents. You review all the documents provided as proof of source of wealth/funds and determine them to be issued by reliable and independent sources. You therefore decide that no further third party verification of source of funds/wealth is required. You also note that one of the trust bank statements was dated two weeks ago. You note that the address on the bank statement matches the address on the trust deeds. You record that you have verified the address on this basis.
If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You help with winding up the family trust.

Example in practice: Assisting a company to acquire another company

The New Zealand-based director of ABC Limited, an architecture and design company, asks you to help the company purchase a competitor business, XYZ Limited, an interior design service, for $25m. You are interested in how ABC Limited can afford it given it is a medium-sized enterprise that is smaller than XYZ Limited, so you conduct enhanced CDD. You are informed by your customer that ABC Limited has gained some large-scale retirement village design contracts in the previous two years. Its annual turnover increased from $5m to $20m per annum and is expected to rise to $30m in the coming year with many more retirement village fit outs expected to be completed. ABC Limited aims to acquire XYZ to enable it to provide a more comprehensive interior design component for its retirement village fit outs. This would increase the income they can generate as the business expands and retirement village fit out becomes a significant source of income.

Steps to complete enhanced CDD	How this applies to the example
Identify which criteria your customer meets to decide the level of CDD you must do.	ABC Limited is a new customer and has a director in New Zealand but some offshore ownership. You are unfamiliar with the company and it is seeking to undertake a large procurement.
Obtain information about the nature and purpose of the proposed business relationship.	The director describes the intention for horizontal and vertical expansion as outlined in the ABC Limited business plan.
Determine the initial level of ML/TF risk.	You identify that the offshore people with beneficial ownership are based in a country that poses a higher ML/TF risk. You determine the level of risk is high and that enhanced CDD must be conducted.
Identify all relevant persons that need to be identified and gather information about the source of wealth/source of funds.	You gather identity information on all those with a beneficial interest in ABC Limited, including the director in New Zealand and the shareholders offshore. You do some research to ensure that none of the beneficial owners are politically exposed persons; it turns out they are not. You also obtain business accounts audited by an accountant, bank records and tax payment records for the previous two years. You consider these documents to be issued by reliable and independent sources. You also sight and record the retirement village contracts showing expected fit outs and you research the business offering the retirement village fit out contracts to ensure it is a genuine company. To be sure of this, you contact them to ensure the contracts you hold remain valid.

Verify the identity information gathered using more in-depth processes than those specified in the Amended Identity Verification Code of Practice[99] because you have determined the level of risk to be high.	You verify the identity of the director of ABC Limited in New Zealand by sighting his passport, his driver licence, a credit card with a New Zealand registered bank, a recent bank statement and a utility bill. For the overseas beneficial owners, you are concerned that obtaining a certified copy of their passports by a lawyer of their choosing does not provide you with the level of assurance you require. However, you are recommended a law firm in that same country that is known to be trustworthy. As a result, you arrange for the beneficial owners to visit and have their passports and other identity information certified by a lawyer in that law firm, who then provides you copies of the certified documents.
If the identity information and verification requirements are satisfied, then you can proceed with the customer's instructions.	You help ABC Limited to purchase XYZ Limited.

Identifying if a customer is a politically exposed person

As soon as possible after establishing a business relationship, or conducting an occasional transaction or activity, lawyers and conveyancers are required to take reasonable steps to identify whether their customer (or any beneficial owner) is a politically exposed person (PEP).[100] The Act requires reporting entities to conduct enhanced CDD if it establishes a business relationship with a customer or beneficial owner who is a PEP, or if a PEP seeks to conduct an occasional transaction or activity through the reporting entity.[101]

A PEP is defined in section 5(1) in the Act.[102] In summary, a PEP is a person, or an immediate family member or someone who has close business ties to that person, who holds or has held (in the preceding 12 months) a prominent public function in a foreign country. This may be because they are or were a head of state, senior politician, or an official with a public profile, such as a Supreme Court Judge, or a highly ranked military official. It could also be because they had authority and influence in a state enterprise in any country. PEPs can be exposed to bribery or corruption or their respected status may be misused (knowingly, or unknowingly) to legitimise otherwise suspect transactions.

If you determine that your customer or a beneficial owner is a PEP, you will require senior management approval to continue the business relationship.[103] Also, you must obtain information about the source of wealth or funds and verify that information.[104] If you have undertaken an occasional transaction or activity for someone who you didn't realise is a PEP, as soon as you can after the transaction you also need to obtain and verify information about their source of wealth or funds.

The *Enhanced Customer Due Diligence Guideline* has more information about how to manage compliance where customers are identified as PEPs.[105]

Wire transfers

The supervisors have published guidance on compliance matters when participating in wire transfers.[106]

A "wire transfer" is a transaction carried out on behalf of a person through a reporting entity by electronic means with a view to making an amount of money available to a beneficiary at another reporting entity (the person on whose behalf the transaction is conducted and the beneficiary can be the same person). An "international wire transfer" is a wire transfer where at least one of the ordering, intermediary or beneficiary institutions is in New Zealand, and at least one is outside New Zealand.

Section 27 of the Act places specific obligations on "ordering institutions" and "beneficiary institutions" when the wire transfer is equal to or above $1,000. Please refer to "Prescribed transaction reports" on page 23 for an explanation of these terms (both of which are defined in section 5(1) of the AML/CFT Act). It is possible that a lawyer could be either an ordering or a beneficiary institution, in which case they must complete identity and verification requirements in line with the AML/CFT Act.[107]

New or developing technologies, or products that might favour anonymity

People with criminal intentions value anonymity and will continually look for new ways to preserve it while conducting their activities. Section 30 of the AML/CFT[108] Act requires that if a customer is seeking assistance for an activity that involves new or developing technologies, or products, that might favour anonymity you must:

1. Complete standard CDD identity and verification requirements; and
2. Take any additional measures needed to mitigate the risk of the new or developing technology or product being used to commit ML/TF

Both steps must be done before you enter a business relationship or conduct an occasional transaction or activity for your customer.

When you can rely on others for CDD

In some specific circumstances, reporting entities can rely on others to conduct CDD if the other party is either:

- A member of the same DBG
- Another reporting entity in New Zealand or a person in another country that has sufficient AML/CFT systems and measures in place and who is regulated for AML/CFT purposes[109]
- An agent; or
- An approved entity

Relying on a member of your designated business group

A member of a DBG (Member A) can rely on another member of that same DBG (Member B) to conduct CDD if the information is given before Member A has established a business relationship or conducts an occasional transaction or activity for the customer. Any verification information must be able to be given to Member A by Member B as soon as practicable but within five working days of the request. In this scenario, Member A (not Member B) is responsible for ensuring that it is complying with the AML/CFT requirements.

Relying on another reporting entity or a suitably regulated person overseas

A reporting entity can rely on another person for CDD so long as the person:

1. Is either a reporting entity in New Zealand or is a person resident in a country which is regulated for AML/CFT purposes;[110] and
2. Has a business relationship with the customer concerned; and
3. Has conducted CDD to at least the standard required by the AML/CFT Act and:
    - Has provided the reporting entity the relevant identity information before it has established a business relationship or conducted an occasional transaction or activity; and
    - Can provide relevant verification information on request of the reporting entity as soon as practicable but within five working days; and
4. Consents to conducting the CDD and providing all relevant CDD information to the reporting entity

In this scenario, and as above, the reporting entity requesting the CDD remains responsible for ensuring the CDD is conducted in accordance with the AML/CFT Act.

Relying on an agent

A reporting entity may authorise a person to be its agent and rely on that agent to conduct CDD and obtain any information required for CDD records. "Agent" is not defined in the Act; instead, the ordinary principles of agency law will apply.

Relying on an approved entity

Section 33 of the Act enables a business to rely on an "approved entity". There are not yet any prescribed approved entities.

When to conduct CDD

You must conduct CDD (ie, obtain the required identity information and verify that information) on your customer before a business relationship with the customer is entered into, or an occasional transaction or activity is conducted.

The only exception to this timeframe, which would allow verification to be completed after the business relationship has been established, will be where all the following criteria apply:

- It is essential not to interrupt normal business practice
- ML/TF risks are effectively managed through appropriate risk management procedures; and
- Identify verification is completed as soon as practicable once the business relationship has been established[111]

Fast-paced scenarios may be common for some lawyers or conveyancers; however, instances of delaying the verification of customer identity information should be truly exceptional. The reasons for delaying verification should be fact-based, justifiable and recorded.

Ongoing CDD and account monitoring

Under section 31 of the AML/CFT Act, when you are in a business relationship with a customer, you are required to conduct ongoing CDD and ongoing account monitoring. You are required to regularly review any information you hold about the customer and regularly review their account activity and transaction behaviour. The purpose of this is to ensure that the nature and purpose of the business relationship and any transactions relating to that business relationship are consistent with your knowledge of the customer and the customer's risk profile. This regular review will also help you to identify any grounds for reporting a suspicious activity.

Reporting entities are required to develop a process for ongoing CDD and account monitoring for their customers according to the level of risk each customer presents. You should think about the level of CDD that was previously undertaken, and consider the level of risk involved with that customer or their activities and transactions. This means higher-risk customers need to have more frequent and thorough account monitoring than customers deemed to be low or medium risk. The account monitoring conducted should enable you to identify any transaction behaviour that is out of character with your knowledge of the customer, their risk profile and the CDD you have previously conducted.

Compliance obligations when conducting international transactions

An area of general business practice that requires specific mention in your AML/CFT programme is your method of ensuring compliance when conducting or participating in international transactions with multiple parties. This is likely to be different for each firm. This section provides some basic information about how to comply with the Act when dealing with parties in other countries that may or may not have reputable AML/CFT regulation. The supervisors have published the *Countries Assessment Guideline* to help you determine whether a country you are dealing with has effective AML/CFT systems and measures.[112]

There is no definitive list of countries that are deemed not to have sufficient AML/CFT systems and measures, so reporting entities should consider a range of factors when determining the level of risk associated with engaging in a transaction with a country. For example, is the country:

- Subject to international sanctions, embargos or other measures?
- Identified by the FATF as lacking adequate AML/CFT systems and measures?[113]
- Recognised as having supporters of terrorism, or financing terrorism?
- Considered to have problems with corruption (eg, it has a low ranking on the Transparency International Corruption Perceptions Index)?[114]
- Known as a tax haven?
- Associated with production and/or transnational shipment of illicit drugs?

What to do if you cannot complete CDD

If you are not able to complete CDD for a customer, you must neither carry out an occasional transaction or activity for them nor establish a business relationship with them.[115] If you already have a business relationship with the customer, and that business relationship relates solely to captured activities, this must be terminated (you are free to continue providing non-captured services to the customer). This applies to all circumstances where a customer fails or refuses to provide information, data or documents that you have requested, including in relation to enhanced CDD. This also applies if the information, data or documents that the customer provides are inadequate.

You should always bear in mind your obligations under the Lawyers' Conduct and Client Care Rules or the Conveyancing Practitioners' Conduct and Client Care Rules (as applicable). These rules allow a lawyer or conveyancer to terminate a retainer for a range of specified reasons including where a customer gives instructions that would cause the lawyer or conveyancer to breach their professional obligations.[116]

If you are declining to enter into a business relationship or refusing an occasional transaction or activity, you are required to consider whether you need to file an SAR with the FIU.

6. Know the red flags

This section draws on available international information about the vulnerabilities of the legal and conveyancing professions to misuse by criminals. This information should assist your general awareness and your considerations of the risks your business may face from unwittingly facilitating ML/TF. In this section, the term "client" is used in preference to "customer" as the text is from open source material that uses the term "client".

Red flags identified by the Financial Action Task Force

The FATF is an inter-governmental body established in 1989 to set standards and promote effective implementation of legal, regulatory and operational measures for combating ML/TF and other related threats to the integrity of the international financial system.

The FATF provides a range of information and advice for the industries and professions that are affected by ML/TF. In June 2013, it published *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.*[117] The report identifies seven common ML/TF methods that require the assistance of a legal professional and present risk to lawyers who may be misused, even unwittingly, by criminals. Conveyancers also need to be mindful of the ML/TF risks they are exposed to.

The seven methods are:[118]

1. Misuse of client accounts
2. Purchase of real estate property
3. Creation of trusts and companies
4. Management of trusts and companies
5. Managing client affairs and making introductions
6. Undertaking certain litigation
7. Setting up and managing charities

1. Misuse of client accounts

Client accounts can be used as the first step in converting the cash proceeds of crime into other, less suspicious assets. This can permit access to financial institutions as it helps to hide the true source or ownership of the funds and assets and can facilitate buying property, setting up shell companies and onward transfer of the proceeds of crime to other parties. See case studies 1 and 2 in Appendix A.

Red flags to watch out for:

- Client actively avoids personal contact without good reason
- Client asks for unexplained speed
- Use of a disproportionate amount of cash
- Use of client account with no underlying legal work
- Willingness to pay fees when no legal work is undertaken
- Client is known to have connections with criminals
- Significant private funding and the transfers are structured so as to avoid the threshold of reporting requirements
- Aborted transactions after receipt of funds and there is an unexplained request to send funds to a third party

2. Purchase of real estate property

Purchase of real estate is a common outlet for criminal proceeds as it appreciates and can provide a legitimate reason for the appearance and movement of funds. In addition, real estate gives criminals a place to live and enjoy the proceeds of their criminal activities or a place to set up new criminal enterprises. See case studies 3 and 4 in Appendix A.

Red flags to watch out for:

- Transaction involves a disproportionate amount of private funding/cash, which is inconsistent with the socio-economic profile of the client
- Funding from third parties requiring further consideration
- Requests to act for multiple parties without meeting them
- Back-to-back property transactions with rapidly increasing value
- Client changes legal advisor multiple times without good reason
- Parties to a transaction are connected without an apparent business reason

3. Creation of trusts and companies

Trusts and companies can be a convenient way to obscure the origin and ownership of assets, particularly if the trust or company is set up by a lawyer. This approach helps criminals retain control over criminally derived assets so they can enjoy the benefit of them while also distancing themselves from obvious ownership. See case studies 5 and 6 in Appendix A.

Red flags to watch out for:

- Use of an intermediary without good reason
- Attempts to disguise the real owner or parties to the transaction
- Involvement of structures in multiple countries where there is no apparent link to the client or transaction, or no other legitimate economic reason
- Client is known to have convictions or be under investigation for acquisitive crime[119]
- Transactions are unusual in terms of volume
- Involvement of high-risk countries[120]
- Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date with no logical explanation

4. Management of trusts and companies

Criminals will often seek the assistance of a lawyer to manage their trust or company to provide greater respectability and legitimacy to the entity and its activities. Techniques used by criminals include persuading a lawyer to act as a trustee to knowingly, or unknowingly, receive the proceeds of crime, or give the appearance of legitimacy and provide legal services that disguise criminal activities. See case studies 7 and 8 in Appendix A.

Red flags to watch out for:

- There are attempts to disguise the real owner or parties to the transaction
- Client is using false or fraudulent identity documents for the business entity
- Requests to make payments to third parties contrary to contractual obligations
- Client is known to have connections with criminals

5. Managing client affairs and making introductions

The involvement of a legal professional in a transaction or their referral of a client to other professionals or businesses can provide a veneer of legitimacy to criminal activities because of their ethical and professional obligations and general standing in society. See case study 9 in Appendix A.

Red flags to watch out for:

- Client requires an introduction to access banking facilities
- Private expenditure is being funded by a company, business or government
- Client is a politically exposed person[121] engaged in unusual private business given the frequency or characteristics involved
- There is an attempt to disguise the real owner or parties to the transaction
- Finance is being provided by a lender other than a credit institution, without a logical explanation or economic justification

6. Undertaking certain litigation

It is essential that lawyers act in a way to protect the right of access to justice by ensuring people have access to representation in litigation. There have been international cases where criminals have sought to exploit this protection mechanism by conducting sham litigation as a way to launder the proceeds of crime. Sham litigation is where, for example, the subject of the dispute is fabricated, or the subject of the dispute was a contract relating to a criminal activity that no court would knowingly enforce. Funds received via a lawyer's trust account purporting to settle a debt or pay compensation could have the appearance of legitimacy sought by criminals. See case studies 10 and 11 in Appendix A.

Red flags to watch out for:

- Client with known convictions for acquisitive crime
- A party to the transaction has known links to organised crime
- Client and/or debtor are located at a distance from the legal professional
- The litigation is settled very quickly, sometimes before the legal professional has actually written to the debtor
- There is a request for the funds received from the debtor to be paid out very quickly, sometimes to third parties.
- Client is unconcerned about the level of fees

7. Setting up and managing charities

Some charities are set up as a vehicle for fraud while others could be used as a front for financing terrorism. In money laundering cases, the proceeds of crime are funnelled through the charity to launder the money and give the appearance of legitimacy. Legitimate funds can be given to a charity that then disguises the intended use and destination of the funds from authorities so that it can fund terrorist groups, activities and causes. See case study 12 in Appendix A.

Red flags to watch out for:

- Non-profit organisation engages in transactions not compatible with those declared and not typical for that body
- There are attempts to disguise the real owner or parties to the transactions
- Client is related to a person listed as having involvement with a known terrorist organisation

There will be other red flags that legal professionals should be on the lookout for when providing these services to a client. Please see Appendix B for the full list of the 42 red flags defined by the FATF.

Red flags identified by the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe

In October 2014, the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe published *A Lawyer's Guide to Detecting and Preventing Money Laundering*.[122] This report identifies a range of red flag indicators. They are included in Appendix B for your ease of reference.

How to keep up-to-date with changing methods of ML/TF

People with criminal intentions will always seek to stay ahead of authorities and the professionals whose services they wish to misuse. Over time new methods of ML/TF will develop and emerge. The FIU and DIA actively maintain a watch for these new methods and communicate them via the FIU's Quarterly Typology Reports[123] and DIA's newsletters.[124] Reporting entities are encouraged to look at these resources as well as media reports and information from the FATF and other jurisdictions to keep up-to-date with developments in ML/TF methods.

7. Know your AML/CFT supervisor

This section explains the regulatory approach you can expect from DIA.

The role of supervisors

DIA is the supervisor for law firms, conveyancing practitioners and incorporated conveyancing firms that are reporting entities under the AML/CFT Act. The Reserve Bank of New Zealand and the Financial Markets Authority both act as supervisors for other reporting entities. Our role includes monitoring reporting entities for compliance with the Act, providing guidance to reporting entities and investigating and enforcing compliance. This is to ensure that the AML/CFT system operates in a robust manner and that criminals seeking to launder money and finance terrorism are detected and deterred.

Our regulatory approach

We outline our regulatory approach for the AML/CFT system in two publications: the *AML/CFT Supervisory Framework*[125] and *Minimising Harm – Maximising Benefit*.[126] We apply a risk-based and responsive regulatory approach that promotes compliance through a mix of strategies, initiatives and tools. We aim to:

- Make it easy for reporting entities who want to comply
- Help reporting entities who are trying to comply
- Use the full force of the law on reporting entities that refuse to comply

We focus our efforts carefully and deliberately. We use our insight, knowledge and understanding to identify risks and determine interventions to most effectively ensure compliance. While we are fully prepared to escalate our response with enforcement action, we are equally prepared to work with reporting entities in a responsive and educative manner. We are a member of the National Co-ordination Committee, and we work with the other supervisors and the FIU, as well as with other government agencies, industry bodies and reporting entities, to apply a consistent approach to the AML/CFT system.

Monitoring and enforcement

We use a variety of regulatory tools to monitor a reporting entity's compliance with AML/CFT obligations. These include desk-based reviews of reporting entities' documents to test technical compliance, on-site inspections to test effectiveness of implementation of compliance programmes, analysis of annual reports and independent audits.

When we identify reporting entities that are not meeting their obligations under the AML/CFT Act, we consider a number of options. One of these options is a remediation plan with the reporting entity. A remediation plan includes a set of expected outcomes that the reporting entity must complete within a set timeframe. The timeframe includes measurable progress towards meeting the obligations under the AML/CFT Act. In most cases the timeframe and actions are met and the reporting entity progresses towards meeting the obligations.

In response to more serious or deliberate non-compliance, we may decide to issue a formal warning or to accept an enforceable undertaking. Alternatively, we may decide to seek an injunction, or a pecuniary penalty, from the High Court.
In the most serious of cases, civil liability acts that are engaged in knowingly or recklessly are criminal offences. There are a number of further criminal offences – for example, failing to report or keep records relating to suspicious activities, structuring transactions to avoid AML/CFT requirements, and obstructing or misleading a supervisor. Where necessary, DIA will prosecute reporting entities for criminal offences under the Act.

Investigations of ML/TF

In New Zealand it is a criminal offence to knowingly and intentionally engage in, or facilitate any other person to engage in, money laundering[127] or the financing of terrorism.[128] The Police are responsible for investigating and prosecuting ML/TF offences, as well as forfeiture proceedings relating to the proceeds of crime. A robust AML/CFT system, in which reporting entities are conducting CDD, keeping customer and transaction records, and reporting suspicious activities, is an important tool in the collective fight against financial and organised crime.

Territorial scope of the AML/CFT Act

The supervisors have issued guidance outlining their interpretation of the territorial scope of the AML/CFT Act.[129] Even though the AML/CFT Act only has jurisdiction in New Zealand, we strongly encourage reporting entities to report on suspicious activities and transactions that they are party to that occur entirely offshore. For more information about reporting suspicious activity, please see "Reporting to the FIU" on page 22.

8. Know where to get support

Reporting entities can access compliance support from a range of sources:

- Your AML/CFT programme and compliance officer
- DIA as the supervisor
- The New Zealand Law Society, the Auckland District Law Society and the New Zealand Society of Conveyancers
- Independent legal advice
- Open source information from relevant international bodies concerned with AML/CFT

Your AML/CFT programme and compliance officer

Where employees in your business have compliance questions, their first port of call should be your AML/CFT programme. This document should be able to provide answers to basic questions that are likely to arise in your specific business context. As questions arise, it is likely that the AML/CFT programme will need to be updated to include provisions for resolving unanticipated issues and frequently asked questions.

Specific questions should be answered by your compliance officer. Where this approach does not resolve the question at hand, it is important to consider what would be the appropriate next step – seeking support from the relevant professional body, from your supervisor or from an independent lawyer.

Support from your supervisor

We recognise that this is a new compliance system to adjust to, and so we aim to provide proactive support to reporting entities. Examples of the support we provide range from general information and awareness promotion, all the way to specific support where a reporting entity is experiencing difficulty but has a genuine intention to comply. The DIA website provides a wide range of information about how to comply with the AML/CFT Act for reporting entities.[130]

The AML/CFT Act allows supervisors to create codes of practice. A code of practice is a statement of practice that helps reporting entities to comply with the AML/CFT Act. So far, one code of practice has been developed: the Identity Verification Code of Practice. This was developed in 2011 and amended in 2013.[131] It should be read in tandem with the Explanatory Note.[132] There are no current plans to develop more codes of practice, but the supervisors are open to feedback from reporting entities on whether more would be helpful.

Support from your industry bodies

Lawyers and conveyancers are encouraged to keep abreast of the information and education on offer from their representative societies. Lawyers can expect a range of information and compliance support from the New Zealand Law Society. The Auckland District Law Society communicates with their members to raise awareness via articles in their publications and by hosting webinars on the topic. The New Zealand Society of Conveyancers also provides a range of information and support to conveyancers.

When to seek independent legal advice

There will be occasions where lawyers and conveyancers need to seek independent legal advice to ensure they remain compliant with the AML/CFT Act. Supervisors cannot provide legal advice to reporting entities. When you have specific compliance questions about unique circumstances that the supervisor or your professional body cannot reasonably answer, you may need to seek independent legal advice.

Other publicly available information

The Phase 2 Sector Risk Assessment (Phase 2 SRA) is essential reading for lawyers and conveyancers. This resource gives reporting entities the background understanding of the ways ML/TF poses risk to lawyers and conveyancers. The *AML/CFT Risk Assessment and Programme: Prompts and Notes* (Prompts and Notes) guideline outlines the factors to be considered in a risk assessment along with some prompts and things to think about when completing a risk assessment and developing your AML/CFT programme. The Phase 2 SRA and the Prompts and Notes are available on the DIA website.[133]

The FATF has a range of information on its website, both specific to the legal sector[134] and to the New Zealand context.[135] You may be interested to read the FATF's 2013 report *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* and the International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe's 2014 report *A Lawyer's Guide to Detecting and Preventing Money Laundering.*[136] The red flags noted in Appendix B have been taken from these reports.

Support that may emerge in the future

As the AML/CFT system becomes established practice in the legal and conveyancing sectors, it is likely that relevant training establishments will begin to incorporate AML/CFT into curricula. Industry bodies will be a good source of information when new educational supports are in development.

Appendix A: Case studies

The case studies in this appendix provide illustrations of the seven common methods of money laundering identified by the FATF in their publication *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.* The case studies have been paraphrased and summarised for ease of reference. The case studies come from both the FATF report and other open source publications – references are provided in the footnotes. The purpose of including these case studies is to raise awareness of how lawyers and conveyancers have knowingly, or unknowingly, been involved with ML/TF both internationally and in New Zealand.

The seven common methods are:
1. Misuse of client accounts
2. Purchase of real estate property
3. Creation of trusts and companies
4. Managing trusts and companies
5. Managing client affairs and making introductions
6. Undertaking certain litigation
7. Setting up and managing charities

1. Misuse of client accounts

Case study 1: Aborted transactions and transfer of funds without underlying legal work[137]
A law firm was approached by a new client with instructions to assist on a number of asset purchases. The client was dealing with a junior lawyer at the firm who, at the request of the client, supplied her with the account details of the firm before completing CDD on the client or entering into an engagement letter with her. The client did not give any further instructions following the deposit of funds. Subsequently, the client explained that she no longer intended to purchase the relevant assets and asked for the deposited money to be provided to a third party, rather than returned to her personal account.

Case study 2: Use of client account to make a payment for ransom to terrorists[138]
Kidnapping for ransom is a growing source of revenue for terrorist groups, including ISIL. Cash often plays a significant role in kidnapping for ransom. Following the delivery of a ransom payment in physical cash, cash couriers move the cash to the terrorist group. Ransom payments can also be paid through financial institutions, such as banks, exchange houses, insurance companies, lawyers, or alternative remittance systems such as hawala. Kidnapping for ransom is particularly relevant to New Zealand as a kidnapping can occur in one jurisdiction and the ransom payment can be made in another. There have also been examples of funds that have been raised by relatives (on behalf of the victim), through the sale of assets and loans, and through the use of trusts to store the donation for a ransom payment.

2. Purchase of real estate property

Case study 3: Investment of proceeds in real estate[139]
A client deposited the total purchase price, in cash, with his lawyers at the very outset of the engagement with the law firm and well before final agreement was reached on the purchase price for the property. The lawyer's CDD indicated the sum that was deposited was a large amount relative to the client's employment income. The purchase of the property went ahead for a sum smaller than that deposited and the remaining funds were returned to a third party indicated by the client. It subsequently turned out the funds deposited were the proceeds of crime.

Case study 4: Misuse of legitimate businesses[140]
In 1998, Tom was looking to make a profitable property investment. He was told by Mariah, one of the directors of Lotos Ltd, that her company was looking to sell one of its buildings at a low price – US$275,000. Tom told Mariah that he wanted to purchase the property as soon as possible. Mariah had informed Tom that a co-director's name, Pete, would be on the contract as the seller of the building. When Tom went to his notary to sign the deed of purchase he did not question that Pete's name was there given his position as a co-director of the company.

Tom was unaware that the day before the sale, Mariah had already sold the building to Pete (in fact, he was her boyfriend and also a co-director of Lotos Ltd). That sale was for US$42,500, which meant that the resale to Tom had given her a profit of US$220,000, which had then gone into her and Pete's personal accounts. Even though Tom was unaware, his notary noticed that the land records showed the recent sale. In his experience the sale price and timing were very unusual and he decided to inform the FIU. The FIU questioned Mariah and the shareholders and found the shareholders had no knowledge of the first sale. Mariah had swindled the shareholders and the tax authorities and at the time of writing was due to face prosecution and asset confiscation.

3. Creation of trusts and companies

Case study 5: Creation of a private trust to disguise the proceeds of crime[141]
In Country A, an elderly female national from Country B with the appropriate visa consults with a trust lawyer. She found the lawyer's name through an internet search. She asks the lawyer to prepare a trust to handle an inheritance she has in Country B. The trust will be funded via wire transfer from Country B into the law firm's client account in Country A. Country B is a country that scores lowly on Transparency International's Corruption Perceptions Index and is subject to various sanctions programmes.

She will be the trustee and her children in Country A will be the beneficiaries. She asks for a memorandum on tax issues and filing requirements. She also wants an introduction to a certified public accountant and to a banker in Country A.

The type of trust requested by the client is a normal structure familiar to most trust lawyers. The goal of the client seems to be asset management for the benefit of the client's children. While the tax consequences may be complex, the plan is relatively typical and the lawyer agrees to act for the client.

Case study 6: Use of professional intermediaries to facilitate money laundering[142]
A criminal involved in smuggling into Great Britain set up a trust in order to launder the proceeds of his crime, with the assistance of a collusive independent financial adviser and a solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The trust was discretionary and therefore power over the management of the fund was vested in the trustees, namely the criminal, his wife and the independent financial adviser. This example illustrates the complexity of trusts used to hide the origins of funds from any law enforcement scrutiny.

One way in which funds were hidden was through the purchase of a garage. The criminal's daughter, who was a beneficiary of the trust, was given the property by her father and she in turn leased it to a company. The property was eventually sold to this company, the purchase funded by a loan provided by the trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the trust, but in practice to the criminal. Thus the criminal, who had originally owned the garage, probably maintained control despite his daughter's ownership. By controlling the trust the criminal was able to funnel funds back to himself through loaning funds from the trust and receiving payment on that loan.

4. Managing trusts and companies

Case study 7: Lawyer manages trusts used to perpetrate an advance-fee fraud scheme and launder the proceeds[143]

A lawyer at a Chicago law firm set up a trust that was used to perpetrate an advance-fee fraud scheme by his client, Mr Voigt. His client claimed it was a long-standing trust associated with the Catholic Church. He then solicited investments for phoney loans. The lawyer managed the trust and his credentials were publicised to add legitimacy to the trust. He may not have known the trust was fraudulent at first, but this soon became clear to him. Nevertheless, he continued to participate, even providing guarantees to borrowers and maintaining the client account where the advance fees were deposited. He distributed the funds to Mr Voigt and his associates. This was in violation of the contract's terms agreed with the loan applicants and the investors.

Case study 8: Tormex Limited[144]

The Tormex case, which was publicly reported overseas and in New Zealand, demonstrates the layers of people and entities that may be used in shell company formation. In this case foreign bank accounts in the shell company's name were used to move criminal proceeds under the guise of trade transactions with the shell company. Tormex Limited was a New Zealand shell company set up by a New Zealand trust and company service provider, GT Group, based in Vanuatu.

Tormex was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The address listed on the companies register for Tormex was the same virtual office in Auckland listed for GT Group. The nominee director resided in Seychelles, and the nominee shareholder, Vicam (Auckland) Ltd, was a nominee shareholding company owned by GT Group. Vicam was itself substantially a shell company and had also been used as the nominee shareholder for hundreds of other shell companies registered by GT Group. For instance, one of the other shell companies that Vicam was used to facilitate was SP Trading Limited, which was used to charter an aircraft that was intercepted in December 2009 attempting to smuggle arms from North Korea.

The actual business of Tormex was not apparent and was not indicated by the company name. Unusual names that do not indicate the activity of the company is a common indicator of shell companies used to facilitate criminal activity. The Organized Crime and Corruption Reporting Project, a network of East European journalists, reported that, once Tormex was registered on the New Zealand companies register, a power of attorney document was used to transfer the directorship to a Russian national. A bank account was then opened at the Baltic International Bank in Latvia. Journalist enquiries with the man revealed he was unaware of either Tormex or its bank account. His identity had been used without his knowledge as he had sold his passport details. An ex-officer of the Russian tax police told journalists: "There are hundreds of law-firms in Moscow, which specialise in setting up ready-made shell companies for their clients, who want to remain in the shadows. Usually law firms use poor people, who sell them passport details. The sum for one passport may vary from US$100 to US$300."

When the journalists examined bank statements for the Latvian account held by Tormex obtained by lawyers in a Moldova court case, they discovered that during 2007 and 2008 US$680 million was transacted through the account. Analysis indicated the transactions were money laundering transactions carried out under the guise of trading contracts between Tormex Limited and several companies. Trade transactions were conducted with several Ukrainian companies including a state-owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third-party offshore companies. The Organized Crime and Corruption Reporting Project journalists report that using transactions related to cancelled trade orders with legitimate companies is a common money laundering method amongst Russian organised crime.

Transactions were also made with three other New Zealand shell companies – Keronol Limited, Melide Limited, and Dorio Limited – which had also been registered by GT Group using the same nominee director, nominee shareholder and virtual office address as Tormex. The UK's *Guardian* newspaper reported that Tormex Limited, Keronol Limited, Melide Limited and Dorio Limited had been involved in laundering US$40 million for the Sinaloa Drug Cartel based in Mexico. Part of the money laundering process involved the New Zealand shell companies transferring funds to an account held at Wachovia Bank in London linked to the Sinaloa Cartel.

5. Managing client affairs and making introductions

Case study 9: Criminal defence lawyer introduces clients to other professionals to assist with laundering the proceeds of their crime[145]
A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments to mortgages on properties beneficially owned by the drug trafficker. The lawyer received commissions from the sale of these properties and brokering the mortgages. While he later admitted to receiving the cash from the trafficker, depositing it into his trust account and administering payments to the trafficker's mortgages, the lawyer denied knowledge of the source of funds.

6. Undertaking certain litigation

Case study 10: Unexpectedly short procedure[146]
A foreign company retained a lawyer to file a claim against another foreign company. The defendant did not contest the claim, so a default judgement was entered. The defendant immediately paid the sum into the law firm's client account. The defendant even paid the amount in question twice – when the secondment was made, the defendant informed that the second payment was made erroneously and asked the law firm to forward the funds to another subsidiary of the defendant company.

Case study 11: Legal practitioners receive requests for use of client account to recover debts with little or no legal services to be provided[147]
Australian legal practitioners have informed their supervisor, the Australian Transaction Reports and Analysis Centre, about receiving unusual requests from prospective clients particularly targeted at passing funds through solicitor's trust accounts. This included a foreign company requesting legal services involving debt recovery, with the legal firm receiving substantial payments in its trust account from purported debtors (both in Australia and overseas) with little debt recovery work actually being required to be undertaken by the law firm.

7. Setting up and managing charities

Case study 12: Legal professional sets up a charity to provide funding to individuals convicted of terrorist activities[148]
In the Netherlands, a foundation was established by a person related to a member of an organisation whose purpose is committing terrorist offences. This person was not designated on international sanctions. The goal for the foundation was to provide funds to help people who were convicted of terrorist offences. Initially a notary refused to establish the foundation, but a second notary agreed to do so.

Appendix B: Red flags

Two key resources for red flag indicators have been compiled: one by the Financial Action Task Force (FATF) and one by the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe (IBA/ABA/CCBE). This appendix provides their lists out of context of their full reports. The References section on page 55 provides bibliographical details and web links to these resources if you wish further information.

FATF red flags

The FATF identifies 42 red flags in their publication *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*.[149] Lawyers and conveyancers are encouraged to review this list to aid their understanding and future identification of suspicious activity.

▶ Red flags about the client:

The client is overly secret about:

- Who the client is
- Who the beneficial owner is
- Where the money is coming from
- Why they are doing the transaction this way
- What the big picture is

The client:

- Is using an agent or intermediary without good reason
- Is actively avoiding personal contact without good reason
- Is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution
- Holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved
- Provides false or counterfeited documentation
- Is a business entity that cannot be found on the internet and/or uses an email address with a domain part such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact
- Is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections to criminals
- Is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities
- Shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries, and suspicious transaction reports[150] – that is, asks repeated questions on the procedures for applying the ordinary standards

The parties:

- The parties or their representatives (and, where applicable, the real owners or intermediary companies in the chain of ownership of legal entities) are native to, resident in, or incorporated in a high-risk country
- The parties to the transaction are connected without an apparent business reason
- The ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason for the transaction
- There are multiple appearances of the same parties in transactions over a short period of time
- The age of the executing parties is unusual for the transaction, especially if they are under legal age, or the executing parties are incapacitated, and there is no logical explanation for their involvement
- There are attempts to disguise the real owner or parties to the transaction
- The person actually directing the operation is not one of the formal parties to the transaction or the representative
- The natural person acting as the director or representative does not appear to be a suitable representative

Red flags in the source of funds:

- The transaction involves a disproportionate amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile
- The client or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation
- The source of funds is unusual, eg:
  - Third party funding either for the transaction or for the fees taxes involved with no apparent connection or legitimate explanation
  - Funds received from or sent to a foreign country when there is no apparent connection between the country and the client
  - Funds received from or sent to high-risk countries
  - The client is using multiple bank accounts or foreign accounts without good reason
- Private expenditure is funded by a company, business, or government
- Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is normally included in the contract, particularly if no guarantee securing the payment is established, without logical explanation
- An unusually short repayment period has been set without logical explanation
- Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation
- The asset is purchased with cash and then rapidly used as collateral for a loan
- There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested that are not appropriate for the common practice used for the ordered transaction
- Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification
- The collateral being provided for the transaction is currently located in a high-risk country
- There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation
- There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk
- The company receives an injection of capital or assets in kind that is notably high in comparison to the business, size or market value of the company performing, with no logical explanation
- There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (eg, volume of revenue, trade or business; premises; size; knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation
- There are large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons

Red flags in the choice of lawyer:

- Instruction of a legal professional at a distance from the client or transaction without legitimate or economic reason
- Instruction of a legal professional without experience in a particular speciality or without experience in providing services in complicated or especially large transactions
- The client is prepared to pay substantially higher fees than usual, without legitimate reason
- The client has changed advisor a number of times in a short space of time or engaged multiple legal advisors without legitimate reason
- The required service was refused by another professional or the relationship with another professional was terminated

Red flags in the nature of the retainer:

The transaction is unusual, eg:

- The type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting
- The transactions are unusual because of their size, nature, frequency, or manner of execution
- There are remarkable and highly significant differences between the declared price and the approximate or actual values in accordance with any reference that could give an approximate idea of this value or in the judgement of a legal professional
- A non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body

The client:

- Is involved in transactions that do not correspond to his/her normal professional or business activities
- Shows he/she does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested
- Wishes to establish or take over a legal person with a dubious description of the aim, or a description of the aim that is not related to their normal professional or commercial activities, or their other activities, or with a description of the aim for which a licence is required, while the customer does not have an intention to obtain such a licence
- Frequently changes legal structures and/or managers of legal persons
- Asks for short cuts or unexplained speed in completing a transaction
- Appears very disinterested in the outcome of the retainer
- Requires introduction to financial institutions to help secure banking facilities

- Creation of complicated ownership structures when there is no legitimate or economic reason
- Involvement of structures with multiple countries where there is no apparent link to the client or transaction, with no legitimate or economic reason
- Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short space of time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation
- There is an absence of documentation to support the client's story, previous transactions, or company activities
- There are several elements in common between a number of transactions in a short period of time without logical explanations
- Back-to-back (or ABC) property transactions, with rapidly increasing value or purchase price
- Abandoned transactions with no concern for the fee level or after receipt of funds
- There are unexplained changes in instructions, especially at the last minute
- The retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services
- There is a lack of sensible commercial/financial/tax or legal reason for the transaction
- There is increased complexity in the transaction or the structures used for the transaction that results in higher taxes and fees than apparently necessary
- A power of attorney is sought for the administration or disposal of assets under conditions that are unusual, where there is no logical explanation
- Investment in immovable property, in the absence of any links with the place where the property is located and/or of any financial advantage from the investment
- Litigation is settled too easily or quickly, with little/no involvement by the legal professional retained
- Requests for payments to third parties without substantiating reason or corresponding transaction

IBA/ABA/CCBE red flags

Country/Geographic risk:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations
- Countries identified by credible sources (ie, well-known bodies that are regarded as reputable (eg, International Monetary Fund, the World Bank) as:
  - Generally lacking appropriate AML laws, regulations and other measures
  - Being in a location from which funds or support are provided to terrorist organisations, or
  - Having significant levels of corruption or other criminal activity

Client risk:

- Domestic and international PEPs
- Entity, structure or relationships of client make it difficult to identify its beneficial owner or controlling interests (eg, the unexplained use of legal persons or legal instruments)
- Charities and "not-for-profit" organisations that are not monitored or supervised by authorities
- Use of financial intermediaries that are neither subject to adequate AML laws nor adequately supervised by authorities
- Clients who:
  - Conduct their business relationship or request services in unconventional circumstances
  - Are cash-intensive businesses (eg, money-service businesses and casinos), that are not usually cash-rich but generate substantial amounts of cash
  - Have no address, or multiple addresses; or
  - Change settlement or execution instructions

Service risk:

- Where lawyers, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they control
- Services to conceal improperly beneficial ownership from competent authorities
- Services requested by the client for which the lawyer does not have expertise (unless the lawyer is referring the request to an appropriately training professional for advice)
- Transfer of real estate between parties in an unusually short time period
- Payments from un-associated or unknown third parties and payments for fees in cash where this would not be typical
- Consideration is inadequate or excessive
- Clients who offer to pay extraordinary fees for services that would not warrant such a premium

Client's behaviour or identity:

- Client is secretive or evasive about:
  - Its identity or that of its beneficial owner
  - The source of funds or money; or
  - Why it is doing the transaction in the way it is

- Client is:
  - Known to have convictions or to be currently under investigation for acquisitive crime, or has known connections with criminals
  - Related to or a known associate of a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations
  - Involved in a transaction that engages a highly technical or regulatory regime that imposes criminal sanctions for breaches (increasing the risk of a predicate offence being committed); or
  - Unusually familiar with the ordinary standards provided for by the law in satisfactory customer identification, data entries and suspicious transaction reporting or asks repeated questions on related procedures

Concealment techniques:

- Use of intermediaries without good reason
- Avoidance of personal contact for no good reason
- Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction
- Use of false or counterfeited documentation
- The client is a business entity that cannot be found on the internet

The relationship between the client and the counterparties:

- Ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature/reason for connection
- Multiple appearances of the same parties in transactions over a short period of time
- The parties attempt to disguise the real owner or parties to the transaction
- The natural person acting as a director or representative does not appear to be a suitable representative
- The parties are:
  - Native to, resident in, or incorporated in a higher-risk country
  - Connected without apparent business reason
  - Of an unusual age for executing parties
  - Not the same as the persons actually directing the operation

Size of funds:

- There is no legitimate explanation for:
  - A disproportionate amount of private funding, bearer cheques or cash (consider individual's socio-economic, or company's economic, profile)
  - A significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company
  - Receipt by the company of an injection of capital or assets that is high in comparison with the business, size or market value of the company performing
  - An excessively high or low price attached to securities being transferred
  - A large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, the activity of the client or its group companies; or
  - The client or third party contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly

Source of funds:

The source of funds is:

- Third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation
- Funds are received from or sent to a foreign country when there is no apparent connection between the country and the client
- Funds are received from or sent to higher-risk countries
- The client is using multiple bank accounts or foreign accounts without good reason
- Private expenditure is funded by a company, business or government; or
- The collateral being provided for the transaction is currently located in a higher-risk country

Mode of payment:

- The asset is purchased with cash and then rapidly used as collateral for a loan
- There is no legitimate explanation for:
  - An unusually short repayment period having been set
  - Mortgages being repeatedly repaid significantly prior to the initially agreed maturity date; or
  - Finance being provided by a lender, either a natural or legal person, other than a credit institution

References

Courts of New Zealand, (28 September 2017), *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited [2017] NZHC 2363*. http://www.courtsofnz.govt.nz/cases/department-of-internal-affairs-v-ping-an-finance-group-new-zealand-company-limited/?searchterm=Ping An

Department of Internal Affairs, Reserve Bank of New Zealand, Financial Markets Authority, (July 2011), *Supervisory Framework*, DIA, RBNZ & FMA, Wellington. https://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_SupervisoryFramework_FINAL_updated28July2011.pdf/$file/AMLCFT_SupervisoryFramework_FINAL_updated28July2011.pdf

Egmont Group, (2002), *FIUs in Action: 100 Cases from the Egmont Group*, Egmont Group, Toronto. http://www.u4.no/recommended-reading/fius-in-action-100-cases-from-the-egmont-group/

Financial Action Task Force, (June 2013), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals,* FATF, Paris. http://www.fatf-gafi.org/publications/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html

Financial Intelligence Unit, (October 2014), *Quarterly Typology Report First Quarter (Q1) 2014/2015,* FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2014-15.pdf

Financial Intelligence Unit, (January 2015), *Quarterly Typology Report Second Quarter (Q2) 2014/2015*, FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014-2015.pdf

Financial Intelligence Unit, (March 2016), *Quarterly Typology Report Second Quarter (Q2) 2015/2016,* FIU, Wellington. http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2015-16-terrorist-financing.pdf

International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, (October 2014), *A Lawyer's Guide to Detecting and Preventing Money Laundering*. https://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=3DBCE981-598E-45E6-8723-CC89C89E8086.

Endnotes

1. The recent changes were made by the Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2017 (the AML/CFT Amendment Act).
2. "Law firms", "conveyancing practitioners" and "incorporated conveyancing firms" are defined in section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
3. Section 130(c), AML/CFT Act (http://bit.ly/2A2AKj7). There are two other supervisors for other reporting entities: the Reserve Bank of New Zealand and the Financial Markets Authority. References to "the supervisors" in this document refer to all three agencies collectively.
4. While the AML/CFT Act refers to "law firms, conveyancing practitioners, and incorporated conveyancing firms", this guide refers to "lawyers and conveyancers" for ease of reference. You should read these terms to have the same meaning – as defined in section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
5. Sections 58(2)(g) (http://bit.ly/2ly11Dz) and 57(2) (http://bit.ly/2h2nN59) of the AML/CFT Act.
6. AML/CFT Act and Regulations: http://bit.ly/2hpGU5V
7. Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
8. FATF evaluations of New Zealand: http://bit.ly/2nY08F1
9. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, p. 35. Please note, where it refers to STR in the diagram, it means "suspicious transaction report". We now refer to these as "suspicious activity reports" (SARs).
10. For the full text of the activities please see section 5(1) of the AML/CFT Act under the definition of "designated non-financial business or profession": http://bit.ly/2xHGfmy
11. AML/CFT (Definitions) Regulations 2011: http://bit.ly/2hrFYy3
12. AML/CFT (Exemptions) Regulations 2011: http://bit.ly/2lAImH6
13. AML/CFT ministerial exemptions: http://bit.ly/2xCmQU6
14. AML/CFT (Class Exemptions) Notice 2014: http://bit.ly/2zly18h
15. Sections 157–159 AML/CFT Act: http://bit.ly/2zuN9wq
16. Interpreting "Ordinary Course of Business" Guideline: http://bit.ly/2Bh3CEI
17. Section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
18. As at December 2017, no arrangements have been prescribed.
19. Both of these terms are defined in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
20. Section 6, Lawyers and Conveyancers Act 2006: http://bit.ly/2ztIqyK
21. Section 4(1), Real Estate Agents Act 2008: http://bit.ly/2h79rQS
22. Residential Tenancies Act 1986: http://bit.ly/2iYKoQl
23. Land Transfer Act 1952: http://bit.ly/2iq9a8c
24. Section 5, Retirement Villages Act 2003: http://bit.ly/2lJhJQv
25. Section 4(1), Real Estate Agents Act 2008: http://bit.ly/2h79rQS
26. Section 42, AML/CFT Act: http://bit.ly/2yj0ECT
27. Sections 53–57 of the Evidence Act 2006: http://bit.ly/2Ah1n7T
28. Lawyers will note that the "prima facie" test also appears in section 136 of the Search and Surveillance Act 2012 (http://bit.ly/2jvrBZB) and section 67 of the Evidence Act 2006 (http://bit.ly/2zOkIgW).
29. DIA v Ping An Finance (Group) New Zealand Limited (2017) NZHC 2363, paragraphs 64–67: http://bit.ly/2kbWHtz
30. Section 92, AML/CFT Act: http://bit.ly/2hrFIiB
31. Section 159A(1) and (2), AML/CFT Act: http://bit.ly/2xGq1Kv
32. Section 9, AML/CFT Act: http://bit.ly/2iR0JH3
33. Section 56, AML/CFT Act: http://bit.ly/2znn4Dd
34. This will only be possible where the business has no employees. The supervisor expects that if the person who is acting as a compliance officer is not part of the business, there should be a justifiable reason. The reporting entity should be able to demonstrate to the supervisor that the person selected has an appropriate level of access to business information and systems to discharge their duties and the authority to advise the senior management of the business about AML/CFT matters.
35. Section 58, AML/CFT Act: http://bit.ly/2ly11Dz
36. Risk Assessment Guideline: http://bit.ly/2iL7Spp
37. Section 58(2)(g), AML/CFT Act: http://bit.ly/2ly11Dz
38. Sector and National Risk Assessments: http://bit.ly/2ik1tAu
39. Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
40. AML/CFT Guide for Small Financial Adviser Businesses: http://bit.ly/2nb1TyA
41. Financial Intelligence Unit assessments and reports: http://bit.ly/2xGSiAx
42. Sections 56 and 57, AML/CFT Act: http://bit.ly/2znn4Dd and http://bit.ly/2h2nN59

43. Section 57(2), AML/CFT Act: http://bit.ly/2h2nN59
44. AML/CFT Programme Guideline: http://bit.ly/2iS5I7k
45. The CDD requirements are noted in Part 2, subpart 1, AML/CFT Act: http://bit.ly/2A5PJtA
46. Section 49, AML/CFT Act: http://bit.ly/2zEQkFA
47. Section 49A, AML/CFT Act: http://bit.ly/2iFJ1lM
48. Section 50, AML/CFT Act: http://bit.ly/2zdxog9
49. Section 51, AML/CFT Act: http://bit.ly/2znMDn8
50. Section 31, AML/CFT Act: http://bit.ly/2z1eCIX
51. Section 59, AML/CFT Act: http://bit.ly/2xJWm2P
52. Section 60, AML/CFT Act: http://bit.ly/2gQqiUa
53. AML/CFT Act and Regulations: http://bit.ly/2hsgYXt
54. General information about annual reporting is here: http://bit.ly/2kcI8WA
55. Sections 59–59A, AML/CFT Act: http://bit.ly/2xJWm2P
56. Guideline for Audits of Risk Assessments and AML/CFT Programmes: http://bit.ly/2AfTf7m
57. It is up to you to decide if someone is suitably qualified to conduct an audit of your AML/CFT programme. You should be able to explain to the supervisor your rationale for this decision on request.
58. Section 59B, AML/CFT Act: http://bit.ly/2muArvE
59. The AML/CFT Amendment Act 2017 changed "suspicious transaction reports" to "suspicious activity reports".
60. DIA v Ping An Finance (Group) New Zealand Limited (2017) NZHC 2363, paragraphs 64–67: http://bit.ly/2kbWHtz
61. Section 5(1) of the AML/CFT Act (http://bit.ly/2xHGfmy); regulation 5A, AML/CFT (Definitions) Regulations (http://bit.ly/2hbI5p6); Prescribed Transactions Reporting (http://bit.ly/2zkB9RJ)
62. Section 45, Terrorism Suppression Act 2002: http://bit.ly/2iI88oj
63. Designated terrorist entities: http://bit.ly/258MtKq
64. goAML – Financial Intelligence Unit reporting tool: http://bit.ly/2ygOri3
65. Section 46, AML/CFT Act: http://bit.ly/2xCrpxz
66. Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (http://bit.ly/2iQDGvZ) and Lawyers and Conveyancers Act (Conveyancers: Conduct and Client Care) Rules 2008 (http://bit.ly/2zJhM23)
67. Section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
68. Section 32, AML/CFT Act: http://bit.ly/2hjDuF3
69. Designated Business Group – Scope Guideline and Designated Business Group – Formation Guideline: http://bit.ly/2y4KpFa
70. Part 2, subpart 1, AML/CFT Act: http://bit.ly/2A5PJtA
71. Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
72. DIA v Ping An, paragraph 44: http://bit.ly/2kbWHtz Section 5(1), AML/CFT Act (http://bit.ly/2xHGfmy). "Existing customer" refers to any person who was in a business relationship with you immediately before the AML/CFT Act began to apply to the legal and conveyancing professions. The AML/CFT Act applies to lawyers and conveyancers from 1 July 2018.
73. Section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
74. The term "beneficial owner" is defined in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
75. More than 25% is the prescribed threshold for the definition of a beneficial owner. Regulation 5, AML/CFT (Definitions) Regulations: http://bit.ly/2yDVy49
76. CDD fact sheets: http://bit.ly/2Bxp2Pc
77. Beneficial Ownership Guideline: http://bit.ly/2Bxp2Pc
78. Section 11(2), AML/CFT Act: http://bit.ly/2gRumUg
79. Clarification of the position the AML/CFT supervisors are taking with respect of the AML/CFT Act interpretation of a trust as a customer: http://bit.ly/2Bxp2Pc
80. Section 18(2), AML/CFT Act: http://bit.ly/2gS5b3V
81. Amended Identity Verification Code of Practice 2013: http://bit.ly/2k13AxJ
82. Identity Verification Code of Practice – Explanatory Note: http://bit.ly/2k13AxJ
83. Section 14, AML/CFT Act: http://bit.ly/2z2zU99
84. Section 15, AML/CFT Act: http://bit.ly/2zDSNQt
85. Section 17, AML/CFT Act: http://bit.ly/2m1YSjC
86. Beneficial Ownership Guideline: http://bit.ly/2Bxp2Pc
87. Amended Identity Verification Code of Practice 2013 available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
88. Section 18(2), AML/CFT Act: http://bit.ly/2gS5b3V
89. Section 21, AML/CFT Act: http://bit.ly/2zDTeu5
90. Amended Identity Verification Code of Practice 2013 available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
91. See "Compliance obligations when conducting international transactions" on page 39 for more discussion of how to assess whether a country is considered high risk.
92. Toogood J confirmed in paragraph 34 of DIA v Ping An that a transaction that is either complex or unusually large will trigger the enhanced CDD requirements. http://bit.ly/2kbWHtz
93. Section 23(1)(a) of the AML/CFT Act: http://bit.ly/2iFkDBE

94. Section 24(1)(a) of the AML/CFT Act: http://bit.ly/2zXSvDA
95. Enhanced Customer Due Diligence Guideline available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
96. Amended Identity Verification Code of Practice 2013 available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
97. Amended Identity Verification Code of Practice 2013 available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
98. Amended Identity Verification Code of Practice 2013: http://bit.ly/2k13AxJ
99. Section 17(b), AML/CFT Act: http://bit.ly/2m1YSjC
100. Section 22(2), AML/CFT Act: http://bit.ly/2zYaTbY
101. See definition of "politically exposed person" in section 5(1), AML/CFT Act: http://bit.ly/2xHGfmy
102. Section 26(2)(a), AML/CFT Act: http://bit.ly/2A8liTh
103. Section 23(1)(a), AML/CFT Act: http://bit.ly/2ilUTJI
104. Enhanced Customer Due Diligence Guideline available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
105. Wire Transfers: available at Codes of Practice and Guidelines: http://bit.ly/2gQ3Iev
106. Sections 27–28, AML/CFT Act: http://bit.ly/2hRYKyV
107. Section 30, AML/CFT Act: http://bit.ly/2gWmRLD
108. See the supervisors' Countries Assessment Guideline (http://bit.ly/2hOTHPk) or the Basel Index, which ranks countries by AML/CFT risk (https://index.baselgovernance.org/ranking).
109. Please note that law firms and conveyancing practitioners in Australia are not specifically regulated for AML/CFT purposes.
110. Section 16(3), AML/CFT Act: http://bit.ly/2iTi1Da
111. Countries Assessment Guideline: http://bit.ly/2hOTHPk
112. High-risk and non-cooperative jurisdictions: http://bit.ly/1lTBG24
113. The Transparency International Corruption Perceptions Index for 2016 is available at: http://bit.ly/2j3Y63K
114. The Basel Index, which ranks countries by AML/CFT risk, may also be useful: http://bit.ly/2djRNDR
115. Section 37, AML/CFT Act: http://bit.ly/2hydAdM
116. Rule 4.2.1(a), Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (http://bit.ly/2htoGR8) and rule 20.1(c), Lawyers and Conveyancers Act (Conveyancers: Conduct and Client Care) Rules 2008 (http://bit.ly/2jpl3iN)
117. Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals: http://bit.ly/2z6i3ff
118. This section paraphrases content from Chapter 4 of the FATF report Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals. For more information, please see the full report.
119. Acquisitive crime is any crime that produces proceeds of crime.
120. See "Compliance obligations when conducting international transactions" on page 39 for more discussion about high-risk countries.
121. "Politically exposed person" is defined in section 5(1) of the AML/CFT Act: http://bit.ly/2xHGfmy
122. A Lawyer's Guide to Detecting and Preventing Money Laundering: http://bit.ly/2hxRCrb
123. Financial Intelligence Unit (FIU) assessments and reports: http://bit.ly/2xGSiAx
124. AML/CFT news: http://bit.ly/2z7lAd4
125. AML/CFT Supervisory Framework: http://bit.ly/2lHausc
126. Minimising Harm – Maximising Benefit: http://bit.ly/2z669Sy
127. Section 243, Crimes Act 1961: http://bit.ly/2zYeqXU
128. Section 8(1) and (2A), Terrorism Suppression Act 2002: http://bit.ly/2lZbZlE
129. Territorial Scope of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009: http://bit.ly/2nf664p
130. Anti-money laundering and countering financing of terrorism: http://bit.ly/2zbaCoS
131. Amended Identity Verification Code of Practice 2013: http://bit.ly/2k13AxJ
132. Identity Verification Code of Practice – Explanatory Note: http://bit.ly/2k13AxJ
133. The Phase 2 SRA is available on the Sector and National Risk Assessments page (http://bit.ly/2ik1tAu) and the Prompts and Notes guideline is available on the Codes of Practice and Guidelines page (http://bit.ly/2gQ3Iev)
134. Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals: http://bit.ly/2z6i3ff
135. FATF evaluations of New Zealand: http://bit.ly/2nY08F1
136. A Lawyer's Guide to Detecting and Preventing Money Laundering: http://bit.ly/2hxRCrb
137. International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, (October 2014), A Lawyer's Guide to Detecting and Preventing Money Laundering, p. 42.
138. Financial Intelligence Unit, (March 2016), Quarterly Typology Report Second Quarter (Q2) 2015/2016, Wellington, p. 13.

139. International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, (October 2014), A Lawyer's Guide to Detecting and Preventing Money Laundering, p. 42.
140. Egmont Group, (2002), FIUs in Action: 100 Cases from the Egmont Group, Egmont Group, Toronto, p. 59. This case study has been summarised by DIA for brevity and ease of reference.
141. International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, (October 2014), A Lawyer's Guide to Detecting and Preventing Money Laundering, p. 44.
142. Financial Intelligence Unit, (October 2014), Quarterly Typology Report Second Quarter (Q1) 2014/2015, Wellington, p. 7.
143. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, p. 61.
144. Financial Intelligence Unit, (January 2015), Quarterly Typology Report Second Quarter (Q2) 2014/2015, Wellington, p. 9.
145. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, p. 67.
146. International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, (October 2014), A Lawyer's Guide to Detecting and Preventing Money Laundering, p. 45.
147. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, p. 70.
148. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, p. 75.
149. Financial Action Task Force, (June 2013), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, pp 77–82.
150. Please note that since the FATF published this information we have moved from "suspicious transaction reports" to "suspicious activity reports".