Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)

Guide for small financial adviser businesses

In this guide you will find:

Financial Markets Authority
PO Box 1179
Wellington 6140
New Zealand

www.fma.govt.nz

ISBN 978-0-478-36850-5 (print version)
ISBN 978-0-478-36851-2 (electronic version)

January 2012

Who is this guide for?

This guide is designed to help financial advisers working independently or in a small business comply with their obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the AML/CFT Act) and associated regulations (together AML/CFT law).

This guideline is **not** designed to meet the needs of larger, more sophisticated businesses with dedicated compliance staff, or the financial advisers that work for them. The methodologies suggested here are likely to be too simplistic for such businesses. If you have a compliance officer, please speak to him/her about how your business will comply with its obligations.

The Financial Markets Authority (FMA) supervises financial adviser businesses under the AML/CFT Act. However, if you are a financial adviser working for a bank or an insurance company you will most likely be supervised by the Reserve Bank rather than FMA. If you do not know who your supervisor is, please speak to your compliance officer, refer to section 130 of the AML/CFT Act, or contact FMA.

This guideline is not intended to be legal advice, and should not be relied upon as such.

What does this guide do?

This guide discusses the role small financial adviser businesses play in the AML/CFT regime, and how they can begin to comply with their AML/CFT obligations. It focuses on risk assessments, customer due diligence (CDD) and suspicious transaction reports (STR) because they are particularly important obligations under the AML/CFT regime, which affect financial advisers in a unique way.

This is not a comprehensive guide for all obligations under the AML/CFT Act. It should be read together with other guidelines available from FMA, most importantly the AML/CFT Programme Guideline.

Which financial advisers must comply with the AML/CFT Act?

In general, financial advisers who help people invest their money are likely to have obligations under the AML/CFT Act (a business that has obligations under the AML/CFT Act is a 'reporting entity').

There are three broad situations where AML/CFT obligations are likely to apply to financial advisers. If, after reading this material, you are unsure whether you have AML/CFT obligations, please speak to FMA and/or seek legal advice.

People required to be authorised financial advisers (AFAs)
Under AML/CFT law, if you are required to be an AFA by the Financial Advisers Act 2008 (the FA Act), you will be a reporting entity **when** you arrange for another reporting entity (such as a product provider) to provide a relevant service (such as selling a financial product) to your customer.

> **Can you say it in plain English?**
>
> If you're an AFA, you will probably have AML/CFT obligations when you advise a customer to buy certain financial products, and then act as an intermediary for the purchase of these products from product providers.
>
> There are limited situations when AFAs may **not** have AML/CFT obligations. For example, if you are an AFA and you do not act as an intermediary for your customers to buy financial products, you are unlikely to have AML/CFT obligations.

If you are not required by the FA Act to be an AFA, but have become one voluntarily, you may still have AML/CFT obligations, as explained below.

Financial advisers exempt from becoming AFAs may still have AML/CFT obligations

Under the AML/CFT law, if your business provides financial adviser services in respect of a category 1 product, it will be a reporting entity when it arranges for another reporting entity to provide a relevant service to a customer.

> **Can you say it in plain English?**
>
> This means your business may have AML/CFT obligations, even if you are exempt from the requirement to become an AFA because you only provide advice to wholesale customers or give 'class advice' (under the FA Act).

Businesses defined as 'financial institutions' by the AML/CFT Act
Some financial advisers will have AML/CFT obligations because they carry out activities listed under the definition of 'financial institution' in the AML/CFT Act.

If you carry out any of these activities in the ordinary course of your business, you will have obligations under the AML/CFT Act. This means that if you are classified by the FA Act as carrying out a 'broking service' or a Discretionary Investment Management Service (DIMS), you are likely to have AML/CFT obligations.

> **Can you say it in plain English?**
>
> This means you are likely to have AML/CFT obligations if you carry out transactions with customer funds, or directly manage client assets.

What is money laundering and terrorism financing?

Criminals launder their money so they can use it without raising suspicion. Money laundering is therefore important for people that profit from criminal activity, such as drug dealers, thieves and fraudsters.

Money laundering is a process. As financial advisers, you should look out for:

People trying to place illegally obtained money into the financial system. Financial advisers who accept customer funds, especially cash, are vulnerable to this. They need to ask questions like "where did the funds come from?"

People breaking up funds and/or moving them around to make it difficult to identify their original source. This is called 'layering'. Because financial advisers offer many different financial products they are vulnerable to it. Look out for transactions that seem unnecessary, uneconomic or that don't match the customer's profile.

People pooling funds, and taking them out of the financial system to use. By this stage the funds will appear legitimate, so it is probably too late!

Terrorist financing involves similar techniques to money laundering. The purpose is to avoid detection by authorities and to protect the identity of the people funding terrorists, and the terrorists themselves. The key difference is the funds involved in terrorist financing may be legitimate (ie not the proceeds of crime). Measures that detect terrorist financing can be an effective way to protect society from terrorism.

If you are an AFA, then your business is the reporting entity

If you are a reporting entity because you are an AFA, it is likely the business you provide advisory services through will also be a reporting entity. Under AML/CFT law, it is possible for your business to discharge your compliance obligations for you.

What does this mean for me?

If you are an AFA, the business you provide services through is best-placed to manage your AML/CFT compliance obligations (eg risk assessment). This avoids duplicating your compliance obligations. It means a business can collectively fulfil the obligations of all its AFAs (for the services they provide through it).

This means, for example, that if you work for a small financial adviser business that employs you and another AFA, both of you can work together to satisfy your AML/CFT obligations.

We have designed this guideline to be read by all the affected financial advisers in a business, so that together they can understand the AML/CFT law and how to comply with it.

If you are a **sole trader** the obligations will apply to you under your trading name.

Why are financial advisers important for AML/CFT?

Financial advisers are the main point of contact between the public and financial product providers. Financial advisers generally meet and establish relationships with their customers, whereas product providers may not. Financial advisers are therefore in a very good position to conduct customer due diligence (CDD).

Financial advisers also have a unique overview of their customers' financial activities. If a customer buys financial products from a range of providers with no apparent economic purpose, the activity may not appear suspicious to each individual product provider. But it may be suspicious to the financial adviser because of the wider view he/she has of a customer's financial activity.

What does this mean for me?

Organised crime, fraud and terrorism are global problems, with serious social, economic and political impacts for every country in the world, including New Zealand. By implementing AML/CFT measures into your business, you can play a part in combating these problems.

How does a 'risk based' regime work?

The AML/CFT regime in New Zealand is '**risk based'**. This means that each reporting entity must assess the risk its own business faces from money launderers and terrorist financers, and develop and apply suitable policies, procedures and controls to detect and deter them. Resources can be targeted efficiently at high risk areas, minimising the cost of compliance for your business.

What does this mean for me?

If your business is relatively small, with only lower risk customers and/or products (for example a firm consisting of two AFAs, with well known customers, whom you offer relatively simple products to), the risk-based regime means your risk assessment and AML/CFT programme can be relatively short and simple.

Financial Advisers' key AML/CFT obligations

By June 2013, if you have obligations under the AML/CFT Act your business must have in place:

- A written risk assessment
- An AML/CFT programme, which includes your policies, procedures and controls for:
    - Managing and mitigating the risks identified in your risk assessment
    - Vetting of staff (if you have any)
    - Training of relevant staff
    - Applying appropriate customer due diligence (CDD)
    - Suspicious transaction reporting (STR)
    - Ensuring adequate records are kept
    - Keeping your programme up-to-date
    - Preventing products and/or transactions that favour anonymity being used for ML/FT
    - Ensuring your business adheres to its AML/CFT programme
    - The review and audit of your AML/CFT programme

Below is an explanation of some of your key AML/CFT obligations.

Risk assessment

A risk assessment is the first step your business must take to comply with the AML/CFT Act. In your risk assessment you will **identify** and **assess** the ML/FT risks your business reasonably expects to face. This will enable you to develop a programme to mitigate this risk in a proportionate way.

This guide describes how a small financial adviser business may go about this in a simple way. If you would like more information please refer to the Risk Assessment Guideline (or refer to external information sources such as ISO NZ/Australia Risk Management guides).

Your risk assessment must:

- be in writing;
- include a description of how you will keep it up to date;
- identify the ML/FT risks your business reasonably expects to face, having regard to factors set out in section 58(2) of the AML/CFT Act;
- enable you to determine the level of risk involved in relation to obligations under AML/CFT law; and
- enable you to prepare an AML/CFT programme to manage and mitigate your risks (section 59 of AML/CFT Act).

Why do I need to work out risk levels?

Your risk assessment must enable you to work out a 'level of risk' for areas of your business, including customer types. This will tell you what CDD is required (in addition to the mandatory requirements of the AML/CFT Act) in a particular situation. Most importantly, your risk assessment will tell you, depending on the situation:

- what steps to take when verifying the identity of the customer, its beneficial owner (if the customer is not a natural person); and representative (if it has one);
- when to carry out enhanced CDD, and when simplified may be ok (in all other situations standard CDD is required); and
- what account monitoring and ongoing CDD is required.

Subject to these mandatory considerations, you can choose to comply with section 58 of the AML/CFT Act in whatever way you think is appropriate for your business. Below is a methodology suitable for a small financial adviser business.

Step 1 of a risk assessment:
Identifying what ML/FT risks your business is likely to face

Identifying your ML/FT risks requires you to carefully consider how each aspect of your business is vulnerable to money launderers or financers of terrorism.

To do this you should rely on your understanding of your business, your business experience, and information published by AML/CFT Supervisors and international organisations such as the Financial Action Task Force (FATF).

Are you an AFA?

If you are an AFA, you will have already completed an Adviser Business Statement (ABS). Much of the information in your ABS (and the ABS of any AFA who is employed by the same company as you) will be useful when considering your business' AML/CFT risks and writing this part of your risk assessment. You may even be able to use parts of your ABS verbatim in your risk assessment.

Section 58 of the AML/CFT Act requires you to consider the following factors (please note the explanations provided below are not exhaustive, but rather to give you an idea of the type of issues to consider. More detail is provided in the Risk Assessment Guideline).

Factors you must consider when identifying risks (section 58(2) of the AML/CFT Act):

The nature, size and complexity of your business:
Some businesses are more likely to be used for ML/FT than others. For example, businesses that accept cash from the public are at more risk than those that only accept cheques or bank transfers. As a financial adviser, you should consider the ability of your customers to use your business to spread their funds across numerous products in order to avoid detection by product providers.

The products and services your business offers:
Pay close attention to any products or services you offer that may allow your customers to hide their identity or move funds in a way that is hard to trace (for example products/services that allow movement of funds in a rapid or complex manner, or across borders). Products/services that can be purchased with cash or in a manner that avoids your CDD processes are inherently high risk.

The way your business delivers its products and services:
Again, pay close attention to any delivery methods that may allow your customers to hide their identity or move funds in a way that is hard to trace. Products delivered via non face-to-face methods (eg the internet), via third parties, across borders or which allow rapid movement of funds are especially vulnerable. Special consideration should also be given to products which are commission-based and/or may incentivise employees to overlook AML/CFT requirements.

Factors you must consider when identifying risks (section 58(2) of the AML/CFT Act) cont:

The types of customers your business deals with:
Some customers should be considered higher risk of being involved in ML/FT because of the industry they are in, for example, customers who have cash intensive businesses or deal in precious metals. High net worth individuals in certain circumstances may be considered a higher risk. Politically exposed persons (PEPs) are higher risk too, especially if from a country associated with corruption (check the Corruption Perception Index) etc. Others may be higher risk because of their legal structure.

The countries your business deals with:
Higher risk countries include, for example, those associated with high rates of corruption or terrorism. Countries with few AML/CFT laws, and/or which do not belong to the FATF, and/or tax havens are likely to present a higher risk too. A joint AML/CFT Supervisors' Countries Assessment guide will be released in early 2012 with further information on this. FATF maintains a list which will be useful for you, as do private firms (for a fee).

The end result of your risk identification process will depend on the size, complexity and nature of your business. Don't consider each aspect of your business by itself. Rather, try to imagine how a possible client could use the services and products your business offers, in the way your business offers them, to launder money or finance terrorism. This means thinking about each aspect of your business in relation to the rest of the business.

One way to identify your risks:

1) Write a list of all the types of customers, institutions, products and services, delivery methods, and countries your business deals with.

2) Next, while reading each of the 'factors you must consider' above, ask yourself (and record the answers):

What is it about the **nature, size and complexity** of your business that makes it vulnerable to ML/FT? Write this above the list, as it relates to all products / delivery methods etc.

Of the **products and services** your business offers, which ones, when considered with the rest of your business, are vulnerable to ML/FT? Note the reasons each product / service is vulnerable alongside the product / service (do this with all factors below, too).

How does the way your business **delivers its products and services** make it vulnerable to ML/FT?

Do you have relationships with any **financial institutions** that may make it vulnerable to ML/FT (eg 'shell' companies or institutions from poorly regulated countries)?

Of the **countries** your business deals with, which are considered to be corrupt / to have low AML/CFT standards / to be associated with profitable crime or terrorism? If you don't know about a country, you may wish to err on the side of caution and treat it as higher risk.

Of the **types of customers** your business deals with, taking into account all of the above, which are more likely to be able to launder money or finance terrorism through your business?

Step 2 of a risk assessment:
Assessing the risks you have identified

Once you have identified the ML/FT risks you expect to encounter in your business, each risk needs to be assessed in terms of a combination of:

- the likelihood the risk will eventuate (ie that this area of your business will be used for ML/FT); and
- the consequences if it does (ie the loss or severity of damage that may result).

How likely is it that the risks you have identified will actually occur?

Some risks you have identified will be more likely to eventuate than others. Risks that are more likely to occur should be treated differently from risks that are less likely to occur.

Consider each of the areas of your business you identified in Step 1 and give it a rating based on how likely it is this risk will occur (ie how likely is it that this customer type / product / service / delivery method etc will be involved in ML/FT?). For example, you could rate each area as either very likely, likely or unlikely to be used for ML/FT.

This likelihood rating could correspond to something like:

Unlikely	Likely	Very likely
There is very little chance of ML/FT occurring in this area of your business (perhaps less than 1% of such transactions).	There is a moderate chance of ML/FT occurring in this area of your business (perhaps up to 10% of such transactions).	There is a high chance of ML/FT occurring in this area of your business (perhaps above 10% of such transactions).

When assessing the likelihood of your business being used for ML/FT, **do not** factor in any current business practices which reduce or mitigate your risks (such as asking for identification, or checking transactions over a threshold). The likelihood rating is about the chance of a money launderer or financer of terrorism trying to use your business. It reflects the chances of ML/FT occurring before any controls are taken into account (ie it only assesses the risk based on who you deal with / what you offer them / how you offer it etc).

Your current controls and practises (if you choose to keep them) are important, of course, when managing your business' ML/FT risks. Once you have completed your risk assessment, it is these controls, along with any new controls that you implement, that will allow you to reduce, manage and/or mitigate these risks to a level which is acceptable to you (and above the minimum standards imposed by law).

An example of this is below.

How serious are the consequences if ML/FT occurs in these areas of your business?

You can think of consequences in terms of how it may affect your business and the damage it could cause your community.

Some risks will have more severe consequences, if they eventuate, than others. For example, a transaction that launders hundreds of millions of dollars is likely to cause more damage than one that involves merely hundreds of dollars. Where possible, you should

apply more stringent policies, procedures and controls to risks with more severe consequences than those with less severe consequences.

What does this mean for me?

For financial advisers, measuring AML/CFT consequences may not be easy. If you have customers that try to launder funds through your business, it is unlikely they will tell you of the criminal activity that generated the funds, or what activity it will enable in the future.

However, you can still assume the more serious the possible criminal activity involved and the greater the amount of money involved, the more serious the potential harm will be for your business and community.

For example, if your business is used by a customer to hide large profits from serious crime, this could make national news, and significantly damage your reputation with customers and product providers. The criminal activity it facilitates could hurt your community and damage your industry's reputation and New Zealand's reputation abroad. You may also face regulatory sanction for not implementing proper AML/CFT controls.

See below for an example of how you could factor consequences in to your assessment.

Calculating the risk level

At the end of this process, you must record a level of risk for each identified risk area, taking into account all the information. Risk levels could, for example, be *Low, Medium or High*.

Review and audit of a risk assessment

You must review your risk assessment to make sure it is up-to-date and effective

Under section 58 of the AML/CFT Act you must describe how you will keep your risk assessment current. You could do this by writing down how you plan to stay up-to-date with ML/FT methods (for example by checking updates on the websites of organisations like FMA or FATF), and how you will change your risk assessment if ML/FT methods change in a way that affects the risks your business faces.

Under section 59 of the AML/CFT Act you must also review your risk assessment to identify any deficiencies in it. If you identify any problems you must address them.

You must get your risk assessment audited

Under section 59(2) of the AML/CFT Act, you must ensure that your risk assessment is audited every two years, or at any other time FMA requires.

The auditor must have relevant skills or experience. This does not necessarily mean they have to be a Chartered Accountant or qualified to undertake financial audits. (For example, people with AML/CFT or relevant financial experience might be suitably qualified.)

The auditor must also be independent, and not involved in the development of your risk assessment, or the establishment, implementation or maintenance of your AML/CFT programme.

AML/CFT programme

Once you have completed your risk assessment, you can prepare an AML/CFT programme. An AML/CFT programme is a record of the policies, procedures and controls you have in place to manage the risks you've identified in your risk assessment and comply with your AML/CFT obligations.

Please refer to the detailed AML/CFT Programme Guideline when developing your programme. It explains and provides information relating to how you should develop polices, procedures and controls for:

- CDD;
- suspicious transaction reports (STRs);
- training;
- vetting (if you are the only employee of your business vetting is not necessary);
- record keeping;
- managing and mitigating the risk from ML/FT; and
- monitoring, examining and keeping written findings.

You must designate an employee as an AML/CFT compliance officer (if you are the only employee of your business, then you can be the compliance officer).

Customer due diligence (CDD)

Your policies, procedures and controls for conducting CDD will form part of your AML/CFT programme. We discuss CDD in detail here because financial advisers have a unique role to play in conducting CDD in our financial system. An understanding of it is also essential to carrying out and implementing a risk assessment.

What is CDD?

CDD is the process through which you develop an understanding of your customers. You must conduct CDD on customers before you arrange for them to purchase any financial products. Note you must conduct CDD on:

- the customer and any person acting on behalf of a customer; and
- any beneficial owner of a customer (this means any individual that owns 25% or more of the customer and/or has effective control of the customer).

CDD is the cornerstone of the AML/CFT regime. It is the best way to prevent your business from being used for ML/FT. Money launderers and terrorist financers can only use the financial system successfully if they can mask their identity, and/or the origins of the funds, and/or the identity of the beneficiaries of the funds.

Are you an AFA?

If you are an AFA, you will already conduct some CDD in order to understand your customers' business, investment needs and goals, and properly advise them (and fulfil your obligations under the FA Act).

The AML/CFT Act extends AFAs' obligations in this area. This means, for example, that instead of just asking where a customer derives his or her income, you must also ask who the beneficial owner of the income is. You will also have to identify anyone that has control of the funds. You must then verify all relevant information given to you.

CDD and your product providers

The providers of any financial products you arrange for your customers to purchase may need to use the CDD information you have collected to meet their own AML/CFT obligations. If you arrange for a customer to buy a product from a product provider, and collect inadequate CDD information on this customer, the product provider can also be liable for any breaches of AML/CFT law. This means product providers are likely to have a keen interest in the AML/CFT systems of any financial advisers who sell their products.

Your product providers may have their own policies and procedures to ensure that when you sell their products you collect sufficient CDD to meet *their* requirements. It may make sense for you to check your product providers' CDD policies (if they have any) while developing your AML/CFT programme. Your AML/CFT programme can refer to obligations that are set by your product provider.

Levels of CDD Under the AML/CFT Act, you must decide the level of CDD appropriate for each customer. There are three levels: standard, enhanced and simplified.
Standard CDD will be the norm. For many of your customers, it may be sufficient.
Enhanced CDD is required where your risk assessment indicates a high risk level. In addition, the AML/CFT Act requires enhanced CDD for certain customer types (such as trusts), and customers that purchase certain products (such as new technologies that favour anonymity).
Simplified CDD will be a rare exception for most financial advisers (used when dealing with government departments, for example).

It is important that you understand when enhanced CDD should be conducted. It may only be a small step up from standard CDD and can often be covered off during an initial client meeting.

More information is available on CDD in the Amended Identity Verification Code of Practice 2013 and from FMA.

How does my risk assessment fit in with my AML/CFT programme and CDD?

A key role of your AML/CFT programme is to set out your policies, procedures and controls for managing your AML/CFT risks.

The programme will set out what level of CDD you will apply to a new customer. You only have to conduct further CDD on an existing customer if you have (or should have) reasonable grounds to suspect that the CDD you have for them is inadequate.

In your risk assessment you will decide on the risk of ML/FT posed by various customer types and products etc in the context of your business. This means when your business signs on a new customer, your programme should set out the information you will collect from this customer based on the risk they pose. The programme will also advise the identity verification documents required.

So, for example, where you have assessed the risk level of a particular customer as high, your programme should ensure you carry out enhanced CDD. See below for example.

Suspicious transaction reporting (STR)

Under section 40(1) of the AML/CFT Act, if a person conducts or seeks to conduct a transaction through your business, and you have reasonable grounds to suspect the transaction or proposed transaction is or may be involved in criminal activity or money laundering, you are obliged to make a suspicious transaction report (STR) to the New Zealand Police Financial Intelligence Unit (FIU).

The FIU uses these reports to assist with investigations into serious crime, money laundering and the financing of terrorism. 'Following the money trail' is a very valuable tool in criminal investigations. It is often the information from an STR that provides a vital lead in an investigation.

A transaction doesn't have to be completed before you can notify the FIU. You can submit STRs to FIU about proposed transactions as well. For example, if you turn a customer away because you are not comfortable with the story they gave you about the source of their funds, you should still submit an STR with the information you have collected.

When you do submit an STR your identity is protected. STRs are stored in a secure database that can only be accessed by FIU staff. The FIU will protect your identity and not forward your personal details when financial intelligence is sent out for investigation.

If you act as an intermediary for product providers, you will probably oversee the completion of application forms and collect CDD which you will then forward to the relevant product provider. If you have a suspicion, you should not rely on the product provider to also develop a suspicion. You should make an STR yourself.

How do I know when to make a report?

You don't need to 'know' or 'believe' that a transaction is linked to crime or money laundering in order to submit an STR to the FIU. Identifying suspicious financial activity can be as basic as a 'gut feeling' that your customer isn't being completely honest with you about where their money came from or the reason they are undertaking the transaction.

For financial advisers, it is especially important to look out for customers who seem to be spreading their funds across an unnecessarily large number of product providers in a way that may avoid detection by individual product providers. Also look out for customers moving funds or liquidating investments without a rational or economic reason.

Ensuring you know what ML/FT can look like and how you can identify suspicious transactions is best done in advance. Education is the best way to prevent confusion and complications when a customer tries to use your business for ML/FT. The FIU can provide you with guidance and feedback over the phone, and also have written material available. You can ring the FIU during regular business hours on 04 460 2969 or email fiu@police.govt.nz.

Annual report

Each year, or as otherwise required by FMA, you must file an annual report which details your AML/CFT risk assessment, programme, CDD and other more general information.

This report is essentially information that indicates how you are complying with your AML/CFT obligations, and generally detecting and deterring ML/FT.

The report will be in a prescribed format. Reporting entities will be required to answer a series of questions.

Sanctions for non-compliance with the AML/CFT Act

Subpart 2 of the AML/CFT Act sets out the possible penalties if you fail to comply with the AML/CFT law. These range from a formal warning or enforceable undertakings (this is an undertaking of a certain course of action a reporting entity makes to an AML/CFT supervisor, which is enforceable by law) to serious criminal and civil penalties, including fines of up to $2 million dollars and two years in prison.

Example risk assessment

Below is a basic example of a risk assessment for a small financial adviser business (and how it will relate to its AML/CFT programme and CDD)

What is it about the **nature, size and complexity** of my business that makes it vulnerable to ML/FT?
Small financial adviser business with less than 50 clients. Only myself and my business partner (also an AFA) sign-up clients. Accept no cash or funds (no trust account). Can only sign-up clients face to face. *Straight-forward systems. To buy any services or products people must talk to my partner or me. Customers can't trade directly over internet.* *Offer a variety of products from different product providers which may enable a money launderer to evade detection of product provider by spreading funds across many products.*

Types of products and services we offer	**In context of *my* business, is it vulnerable to ML/FT? Why? Why not?**	**Likelihood rating of ML/FT**	**Factors which indicate more severe consequences**	**Risk level, and whether necessitates extra CDD measures**
KiwiSaver	No. KiwiSaver funds difficult to move/use.	Unlikely	No	**Low**
Products that allow rapid movement of funds	Maybe – but have to speak to my partner or me to move funds, so speed limited	Likely	No	**Medium.** Ask additional questions when customers use these services and verify answers. Enhanced CDD if anything suspicious

Countries we deal with	**Is it considered higher risk? Why?**	**Likelihood rating of ML/FT**	**Factors which indicate more severe consequences**	**Risk level, and whether necessitates extra CDD measures**
New Zealand	No	Unlikely	No	**Low**
Australia	No	Unlikely	No	**Low**

North Korea	Yes, due to high levels of corruption / international financial crime	Very likely	Notoriety of North Korean issues may make it newsworthy	**High**. Conduct enhanced CDD on customers from this country

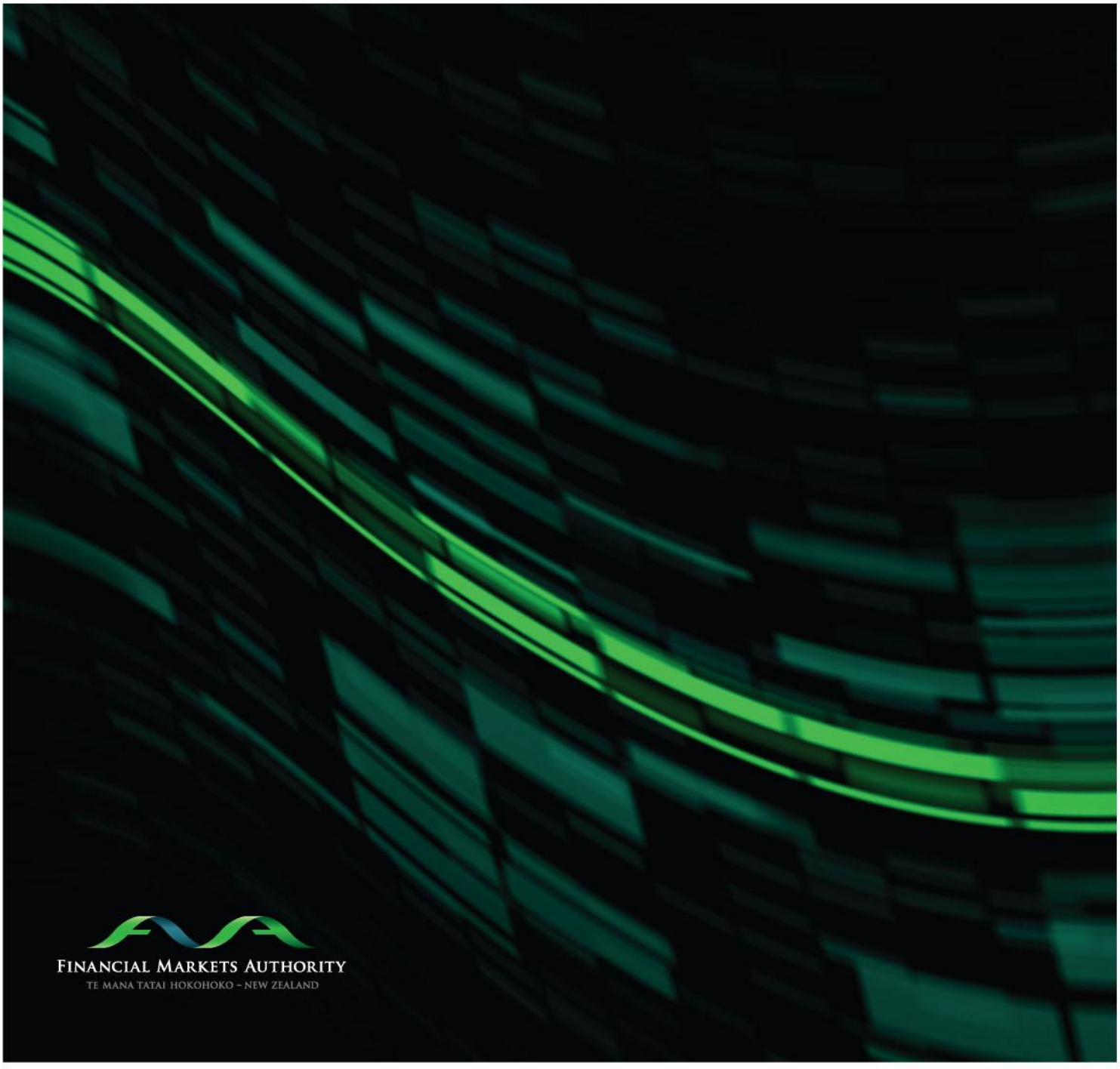
The institutions we deal with	**In context of my business, does it pose a risk? Why/why not?**	**Likelihood rating of ML/FT**	**Factors which indicate more severe consequences**	**Risk level, and whether necessitate extra CDD measures**
Major NZ and Australian based banks	No. All have good AML controls	Low	No	**Low**

Types of customers we deal with	**In context of my business, does it pose a risk? Why/why not?**	**Likelihood rating of ML/FT**	**Factors which indicate more severe consequences**	**Risk level and CDD action required (and additional monitoring etc)**
Typical small investor, with average income etc (stereotype 'ma and pa' investor)	No. Nothing to indicate any risk	Unlikely	No	**Low.** Standard CDD. Review activity if outside the norm, or start using high risk products
Individual who derives substantial profit from a cash intensive business (eg second hand dealer)	Yes, due to amount of money involved and cash nature of business	Likely	Large amounts of cash may indicate serious crime. Also may catch media attention	**High.** Enhanced CDD. Review activity every 6 months, investigate any unusual transactions
Some local, non-complex companies. None are shell companies or otherwise higher risk	No. Nothing to indicate any risk	Unlikely	No	**Low**

Where to from here?

The sooner you begin working on your AML/CFT obligations, the easier it will be to comply with the AML/CFT Act. In particular, we strongly recommend you begin your risk assessment as soon as possible.

Check FMA's website www.fma.govt.nz for useful reference material, guidance and updates relating to the regime. If you do not receive a quarterly update from FMA and would like to, please contact FMA at aml@fma.govt.nz.


FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND