Preparing for AML/CFT: Part 1

What is it?
What are we doing about it?
What do you have to do about it?

Overview

• What it is
• The impact in NZ
• The AML/CFT Act
• Who does what
• Your obligations
What is it?

Money laundering

How criminals disguise the illegal origins of their money. The objective is to make the funds look like legitimate funds that were obtained through normal transactions such as selling property or gambling at a casino.
Money laundering myths:

- “It’s always physical cash that smells like marijuana” Although this has occurred, in fact much money laundering these days is carried out electronically, for example using funds obtained through on-line fraud. Cash is not always a feature in money laundering.

- It’s always related to drugs. Money laundering can be associated with any serious crime that results in financial gain.

- It’s always an overt operation designed to retain as much of the money as possible – it can just mean spending illegally gotten gains!

### Basic Principles

- Placement, Layering, Integration
- Purchase of valuable assets
- Use of remitters
- Use of banks
- Use of shell companies
- Overly complex transactions
- Transactions that make no financial sense

Generally ML is a three step process involving:

- Introduction of illegally obtained money in the financial system (this step is called “placement”);

- Disguising the audit trail so it is difficult to identify the original source of the funds. This is often achieved by breaking funds up and moving them around in a series of complex transactions (this step is called “layering”);

- Transferring the now apparently legitimate funds into a form which they can be used (this step is called “integration”).

- Frontline people may not see all three steps in the transaction process – its important to be aware of any/all steps.
Phase Description Example

Placement Cash enters the financial system. Proceeds of selling cannabis deposited into a bank account.

Layering Money is involved in a number of transactions. Money is transferred into other bank accounts that have been set up and international travel tickets are purchased.

Integration Money is mixed with lawful funds or integrated back into the economy, with the appearance of legitimacy. International travel tickets are cancelled, which results in a reimbursement cheque being issued to the suspect, minus cancellation fees. Money is used to buy goods and services, property or invested.

Basic Principles

• Use of multiple accounts or identities
• Involvement of countries with poor AML/CFT
• Smurfing
• Unexplained wealth
• Use of trusts, gatekeepers, lawyers
• Use of cash and cash couriers
Basic Principles

• Alternative remittance – hawala
• Trade based money laundering
• Nominees and family members
• Co-mingling and Structuring
• Refinement and currency conversion

500 euro note = about NZ$1000

Banned from sale in UK due to links to organised crime

Refinement from $20s to higher denominations or currencies.
Financing of terrorism

Terrorism financing is “the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts”

Financiers 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. The Internet and globalisation has made this easier.

It’s not just about providing direct support to terrorist acts (like buying bombs), it can just be helping terrorists to live day to day. It’s almost like a mirror image of money laundering - often Terrorism Financing is legitimate/clean funds used to finance crime/terror, Money laundering is laundering the proceeds of crime to make it legitimate/clean.

Good CDD and account monitoring will help to detect areas of risk.
Well yes it does.

- Even NZ with its relative isolation has its own home-grown crime
- With globalisation and the internet, we are increasingly exposed to risks from international organised crime and possibly even from organisations supporting terrorism.

You can find examples of ML risks in NZ in the National Risk Assessment, available on the Ministry of Justice website.
What are we doing about it?

Anti-Money Laundering and Countering Financing of Terrorism Act 2009…

…or AML/CFT Act for short!

Start date: 30 June 2013

Yes, it is a mouthful. That’s why it is know as the AML\CFT Act for short

Commencement Order 2011 brings all obligations under the Act into force on 30 June 2013 – the two year countdown is almost half way through

There won’t be an assisted compliance period like there was in Australia
Detect and deter money laundering and financing of terrorism.

The detection and deterrence of ML and TF is best achieved by you because you best know your business, the risks involved and the customers you deal with. You know what’s a normal transaction and what’s abnormal.

The public/private sectors are working together to ensure criminals do not use NZ businesses for ML or FT.
Ensure NZ is a good international citizen.

There are international standards we are expected to comply with. New Zealand is a member country of the Financial Action Task Force who evaluate our systems and policies for detecting and deterring ML/FT every 4 years or so and we need to show New Zealand is complying with that.

Our credit rating and relationships with other countries (whether they want to do business with us) can be affected if we aren’t responsible.

Maintain public confidence in the financial system.

New Zealanders want to know they’re investing their money with a company that isn’t laundering money for criminals.
Benefits to business

• Improve systems and services
• Keep criminals out
• Protect your ability to do business
• Protect your reputation

We are aware that some of these requirements will mean new costs to your business. But there are also important benefits to all businesses from compliance with the Act – in addition to protecting yourself from enforcement action by your supervisor!

First, many businesses find that doing their risk assessment and setting up their AML programme is not just useful for AML compliance. It also gives them an insight into their business which helps in overall business improvement, including their systems and the services they provide.

Secondly, the AML programme helps you keep criminals out of your business. This means that you are protecting your own business from exploitation, for example by fraudsters who might want to rip you off – as well as doing your bit to protect the public from criminality.

Thirdly, the AML/CFT Act brings New Zealand into line with reputable business practice in the rest of the world. Many countries now have legislation preventing businesses from working with other businesses that are not set up to do AML/CFT properly, or that are in a country that has poor standards of AML/CFT compliance. By complying with the Act you protect your firm’s ability to do business locally and internationally.

Finally, by complying with the Act you protect the reputation and integrity of your business.
International Environment

Shows that it is not just NZ

Roles of Agencies

The Police investigate money laundering and terrorist financing. They also house the Financial Intelligence Unit (FIU)

Analyses the national risk and threat of ML and FT

Collects information on suspicious financial transactions
Monitors large amounts of cash crossing borders

**MOJ**
Administer AML/CFT policy and legislation
Advise Minister on overall effectiveness and efficiency
Convene National Co-ordination Committee
Ministerial Exemptions

Legislation includes the Act and Regulations

Advice to Minister will include any changes necessary to the AML/CFT regime to improve its effectiveness

**Customs**
Duty to prevent movement of cash in breach of Act’s requirements
Collect border cash reports
Can exercise powers under Customs and Excise Act 1996 to achieve this

**Supervisors – FMA, DIA, Reserve Bank**
Monitor and assess sector risk
Monitor, investigate and enforce compliance with the AML/CFT Act
Develop codes of practice and guidance for reporting entities

All these six agencies are working together to put the regime into effect. They meet regularly is to ensure that the necessary connections between the agencies are made in order to ensure the consistent, effective, and efficient operation of the regime. They also work with other agencies such as the Ministry of Economic Development, OFCANZ (the Organised and Financial Crime Agency) and IRD.
• Issuers of securities
• Trustee companies
• Futures dealers
• Collective investment schemes
• Brokers
• Financial advisers

The Financial Markets Authority will monitor these entities.

This includes authorised financial advisors, AML/CFT obligations apply to the AFA’s entity rather than the individual AFA’s
DIA will monitor these entities – plus any others that are captured by the Act and don’t fall within FMA or Reserve Bank’s sectors

**IF ASKED…**

Money service business includes: currency exchange and money remittance/transfer.

Lending includes: non-deposit-taking lenders, debt collection and factoring

Managing means of payment includes: non bank credit card providers

Trust and Company Service providers are those businesses that provide 1 or more of the following activities:

- Acting as a formation agent of legal persons or arrangements
- Arranging for a person to act as a nominee director/shareholder or trustee in relation to legal persons or arrangements
- Providing a registered office, business address, or accommodation, or a correspondence, or an administrative address for a company, a partnership, or any other legal person or arrangement
- Banks
- Life insurers
- Non-bank deposit takers

Non-bank deposit takers are finance companies, building societies and credit unions
Supervisory Powers

All powers necessary to carry out functions including:

- Require production of records, document or information
- Conduct on-site inspections
- Entry, search and seizure
- Cooperate and share information
- Initiate and act on requests from overseas counterpart
- Power to delegate

Civil liability acts

Failure to comply with Act

Sanctions

- formal warnings,
- enforceable undertakings,
- injunctions,
- civil proceedings
- Fines - up to $200,000 (individuals)
- $1 – 2M (body corporate)

Civil liability act – occurs when a reporting entity fails to comply with any of the AML/CFT requirements
Criminal Offences

- Civil liability act if committed knowingly or recklessly
- A number specific to STRs
- Obstructing/providing false information

Penalties

- Up to 2 yrs imprisonment/$300,000 fine (individuals)
- Up to $5M (body corporate)

A reporting entity that engages in conduct constituting a civil liability act commits an offence if the reporting entity engages in that conduct knowingly or recklessly.

STR related offences include:

- failure to report an STR
- providing false/misleading information re STR
- unlawful disclosure of STR
- failure to retain adequate records re STR
- obstructing investigation into STR

A person conducts an offence if they wilfully obstruct any AML/CFT supervisor in the exercise of any of their AML/CFT Act powers/functions and if they provide information to a supervisor knowing that information to be false or misleading in any material respect.
To facilitate and assist with the prevention, detection and investigation of money laundering (ML), serious offences, proceeds of crime and terrorism financing (TF)

This is the key role of the FIU. To facilitate and assist with the prevention, detection and investigation of money laundering, proceeds of crime and terrorist financing.

This is done by collecting, analysing and - if appropriate - disseminating information received from financial institutions in relation to suspected money laundering, proceeds of crime or terrorist financing.

The FIU has grown over the last two years to 19 full time equivalent staff. We are carrying a number of vacancies at the moment, but once we are fully staffed we will have more resource available to be proactive.

FIU and ARUs make up the FCG.
New Zealand FIU

• A police unit - Sworn and non-sworn staff
• Intelligence unit NOT investigative
• National focus/responsibility
• Operational and policy focus – Input into policy and law
• Close relationship with partners
AML/CFT Act & FIU

Responsible for:
- STRs, BCRs & SPRs
- Collection, analysis, dissemination
- Guidance on typologies and obligations
- National Risk Assessment
- Best practice guidelines
- Work with Sectors

AML/CFT Act & FIU

- AML/CFT vs Financial Transactions Reporting Act 1996
- AML/CFT in two phases
- More power to share information
- More power to order information

Section 143 – power to order people to provide information and share it with others
NZ National Risk Assessment

• Aids decision makers in prioritisation and resourcing
• Provides information on typologies
• Anticipate problems and limit consequences
• Sector Risk Assessments

Quarterly Typology Report

• Open source document that provides an update on ML and TF
• Provides information on emerging typologies and case studies
• Financial crime and ML
What do you have to do about it?

You need to be ready to fulfill your obligations from 30 June 2013.

Key requirements

Part 2 of the AML/CFT Act
• Risk assessment
• AML/CFT programme
• Suspicious transaction reporting
AML/CFT Regulations 2011

• Definitions
• Exemptions
• Requirements and compliance
• Ministerial exemption form

The obligations we talk about in this presentation are what apply to most businesses. You should check the Regulations to see if any exemptions apply to your business.

Regulations contain inclusions (e.g., trust and company service providers and authorised financial advisers) and exemptions from all or part of the AML/CFT obligations under the Act.

For example, debt collectors are exempt from all aspects of the regime except suspicious transaction reporting.

You should read and understand the Regulations and how they relate to your business.

MOJ will be consulting on other regulations later this year – including annual report and suspicious transaction report forms.
The AML/CFT Act takes a risk based approach. The Police and supervisors carry out their own risk assessments. The National Risk Assessment (completed by police) focuses on the main methods of money laundering used in New Zealand, and the main risks from a law enforcement perspective. Sector Risk Assessments (completed by each supervisor) focus on risks in each sector associated with particular services and products.

You will also be expected to develop your own risk assessment:

- You know best about your business i.e. what is and isn’t a normal customer
- You know the risks

We strongly recommend you refer to the SRA when conducting your own risk assessment.

We have released a Risk Assessment Guideline to help you with your risk assessment, this includes a list of additional resources that will assist you

FMA has issued a small business guideline to help with risk assessment – available on the FMA website
Risk assessment:
What to look at

- Size and complexity
- Products and services
- Delivery channels
- Customers
- Countries

When assessing the risk your business may be susceptible to you should consider:

- Nature, size and complexity of your business
- Products and services you offer – are they risky – e.g. cash intensive, high risk of anonymity? Could they be associated with ML according to sources such as the National Risk Assessment
- The way you deliver your products and services – e.g. face to face vs online
- The types of customers you deal with – e.g. business relationship/client vs one-off
- The countries you deal with – compliance with AML standards, association with serious/organised crime, ML, drug trafficking, corruption, armed conflict
You must assess and rate the likelihood of your business being used for ML/FT

Consider each aspect you have identified using your business experience and published information

The end result will be a likelihood rating for each at-risk area of your business. You could use the following ratings

- Very unlikely
- Possible
- Likely
- Very Likely

Your risk assessment must enable you to prepare a comprehensive compliance programme

The Risk Assessment must be in writing and describe how the business will ensure the assessment remains up to date
Your AML/CFT programme must include procedures, polices and controls to detect, deter, manage and mitigate ML and TF.

Programme is based on your AML/CFT risk assessment and will include adequate and effective procedures, policies and controls for:

- Vetting and training staff
- CDD requirements
- Suspicious Transaction Reports
- Record Keeping
- How you will mitigate/manage risks of ML and TF
- Account Monitoring

You need to appoint an AML/CFT officer responsible for the risk assessment and the programme, who reports to senior management. Senior management also need to approve the programme.

The AML/CFT Programme guideline is available on your supervisor’s website and discusses the key elements in your AML/CFT programme.
Customer due diligence

Abbreviated as CDD

Customer Due Diligence involves gathering and verifying information about a customer’s:

- Identity
- Beneficial owners
- Representatives (i.e. people acting on their behalf)

The purpose of good customer identification and verification processes is to:

- Manage identity fraud risks and the criminal use of anonymity
- Ensure greater observation of transaction behaviour of higher risk customers
CDD – when?

- New business relationship
- Occasional transaction
- Existing customers

You must do CDD on:

- Customers seeking to establish a new business relationship, e.g. set up an account or take out a loan: or

- Customers conducting an occasional transaction (an occasional transaction means a cash transaction that occurs outside of a business relationship, over the applicable threshold (these are set out in the Definitions Regulations) whether carried out in a single operation or several that appear to be linked.

- Existing customers where there has been a material change in the nature or purpose of the business relationship or if the account is anonymous, or you consider you do not have sufficient information on the customer

- You also have to review your existing customer base periodically to ensure information is complete and up to date – this is ‘ongoing CDD’
CDD – who?

- Customer
- Beneficial owners
- Person acting on behalf of customer

Who to do CDD on:

- A customer (new or existing)
- Any beneficial owner of a customer (individuals who have effective control of a customer or own 25% or more of a customer when the customer is a legal person—a company, trust or other organisation)
- Any person acting on behalf of a customer

There are three levels of CDD that depend on the risk that each customer represents (based on your risk assessment):

- Simplified/standard and enhanced due diligence
Standard CDD requires you to collect identity information including:

- The person’s full name and date of birth
- If the person is not the customer, the person’s relationship to the customer
- The person’s address or registered office
- The person’s company identifier or registration number

You must then take reasonable steps to be satisfied that the above information is correct, verify any beneficial owner’s identity, and if the person is acting on behalf of a customer verify their identity and authority to act.

You must also collect information on the nature and purpose of any proposed business relationship, and gather sufficient information to determine whether the customer should be subject to enhanced CDD.

You must also conduct standard CDD as soon as practicable after you become aware that an existing account is anonymous (requirements and compliance regulations).
The Identity Verification Code of Practice is available on your supervisor’s website. It sets out a standard of practice to help you verify the name and date of birth of customers you have assessed as low to medium risk that are natural persons.

It covers documentary and electronic identity verification including the use of certified documents.

It details acceptable primary photographic and non-photographic identification, and outlines when secondary or supporting identification is required.

For example, a passport on its own, or a driver licence together with an eftpos card.

The Code of Practice also includes a standard for electronic identity verification. This is any form non-face to face identity verification done on-line that doesn’t include a requirement for you to sight identity documents. An example is the igovt identity verification service (RealMe).

We are looking at making some amendments to the Code of Practice to ensure it is compatible with RealMe and any other robust electronic verification processes that may become available.

Effect of the Code of Practice - Although it is not mandatory, it constitutes a safe harbour. If a reporting entity fully complies with the code it is deemed to be compliant with the relevant parts of the legislation. If a reporting entity opts not to comply, it must adopt practices that are equally effective, otherwise it risks non-compliance.
Simplified CDD can be conducted on:

- Government Departments
- Local Authorities
- Crown entities
- Listed companies

Simplified CDD requires you to obtain identity information from the person acting on behalf of the customer:

- Full name
- Date of birth
- Their relationship to the customer

You must verify the identity of the person acting on behalf of the customer, and their authority to do so.

This must be done before establishing a business relationship/conducting an occasional transaction on behalf of the customer.

Obtain information on the nature and purpose of any proposed business relationship.

The difference between simplified CDD and standard CDD is that you do not have to obtain or verify information on beneficial owners for simplified CDD.
You must conduct enhanced due diligence in the following circumstances which have a higher ML/TF risk associated with them:

If you establish a business relationship/conduct an occasional transaction on behalf of a customer that is

- A Trust
- A Non-resident from a country with insufficient AML/CFT systems or measures
- A Company with nominee shareholders or shares in bearer form
- Where new or developing technologies, or new or developing products, that might favour anonymity are involved
- If a customer seeks to conduct a complex or unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose

or

- If the customer is **A Politically exposed person** including:
  - Head of State/country or government
  - Government Minister or equivalent
  - Supreme Court Judge or equivalent
  - Governor of a central bank or equivalent
  - Senior foreign representative, ambassador or high commissioner
• High ranking member of armed forces
• Board chair, CE, CFO or position with comparable influence in any State enterprise
• Includes their immediate family
• Includes anyone in joint ownership with a PEP, or who owns an entity on the PEPs behalf

Any other time you consider that the level of risk involved requires it

Enhanced CDD requires the collection and verification of the same information as standard CDD as well as:

The collection and verification (according to the level of risk involved) of information relating to the source of the funds or the wealth of the customer

Where a customer is a trust, you must obtain the name and date of birth of each beneficiary of the trust, if there are more than 10 beneficiaries, the class or type of beneficiary and if it is a charitable trust – the objects of the trust
Reporting entities must prepare an annual report on the risk assessment and AML/CFT programme and provide it to their supervisor.

The Annual Report must:

- Include the information prescribed by the regulations:
- Take into account the results and implications of your audit

A form for the annual report is likely to be gazetted later this year. We are looking at having the AR submitted on line for those with the capacity.
Reporting entities must review their Risk Assessment and AML/CFT programme to:

- Ensure they remain current
- Identify any deficiencies in their effectiveness
- Make any changes identified as necessary to remedy deficiencies

Must audit Risk Assessment and AML/CFT programme every 2 years (or at request of supervisor)

Supervisors will be issuing guidelines for the audits.
FIU & STRs

- Unusual is a better concept than suspicious
- Reporting entities know their business better than anyone
- Do not need to know what the crime is
- Obliged to report under AML/CFT
- Electronically within 3 days

Suspicious Transaction Reports aren’t a new concept. If you are captured under the Financial Transactions Reporting Act 1996, then you already have an obligation to report any suspicious transactions to the Commissioner of Police.

However you best know what is suspicious in your business! And there is no set list of ‘suspicious’ transactions. There is no minimum transaction value on a suspicious transaction either.

A best practice guidelines document is publicly available for STRs submitted under the FTRA96. Police will be issuing a new set of guidelines on submitting STRs under the AML/CFT Act prior to the ‘go live’ date.

Suspicious Transaction Reports aren’t a new concept. If you are captured under the Financial Transactions Reporting Act 1996, then you already have an obligation to report any suspicious transactions to the Commissioner of Police.

Generally suspicious transactions are:

- Large amounts
- Lots of small transactions
- Transactions across borders
- Behavior that is abnormal for that kind of account
- Transactions that don’t make economic sense
- Money going in and out on the same day
However you best know what is suspicious in your business! And there is no set list of ‘suspicious’ transactions. There is no minimum transaction value on a suspicious transaction either.

A best practice guidelines document is publicly available for STRs submitted under the FTRA96. Police will be issuing a new set of guidelines on submitting STRs under the AML/CFT Act prior to the ‘go live’ date.

Suspicion is not the same as knowledge. You don’t have to be sure that your customer is laundering money or financing terrorism. And you don’t have to know what the ‘predicate’ offence is (e.g. drug trafficking or tax evasion).

But you shouldn’t just report every transaction you are unsure about. That is called defensive reporting and you will receive negative feedback from us if we think you are doing that. If you are in doubt, then call or email us. We cannot make the decision for you, but we can talk you through the process.

---

**FIU & STRs**

What to include in the STR:

- Prescribed Details (to be regulated)
- For now… refer to the FTRA96 regulations as a guide
- Quantitative - the transaction details
- Qualitative - behaviour etc.
- Don’t forget about proposed transactions!
Electronic Reporting

- Manner defined by Commissioner of Police
- Single and batch reporting from reporting entities
- No more paper based (with exceptions)
- Verbal if urgent
- XML schema
- FIU guidelines will be produced
NZ Police Asset Recovery Units (ARUs)

Currently investigating 44 cases where STRs have contributed to or led to the investigation

Cases estimated to have associated assets worth an estimated $86 million

Various offences revealed by the STR including drug offending, tax evasion, money laundering, & fraud
STRs and Asset Seizure

Operation ARK

arrest of organised criminal group responsible for manufacture & supply of 90% of the NZ ecstasy market

assets worth an estimated $18 million restrained pending further investigation & legal action

assets included cars – including a bentley, houses, cash, bank accounts

also seized firearms, pills, and pill presses
Did you receive our quarterly e-newsletter, if not contact us and let us know.
Questions?