Improving New Zealand's ability to tackle money laundering and terrorist financing

Ministry of Justice consultation paper on Phase Two of the AML/CFT Act

August 2016

MINISTRY OF JUSTICE
Tāhū o te Ture

New Zealand Government

Contents

Glossary

AML/CFT	Anti-money laundering and countering financing of terrorism
CDD	Customer due diligence
DBG	Designated business group
FATF	Financial Action Task Force
FIU	Financial intelligence unit of NZ Police
ML/TF	Money laundering and terrorist financing
STR	Suspicious transaction report
Reporting entities	Businesses subject to obligations under the AML/CFT Act

Part 1: introduction

Overview

We are seeking feedback about proposed changes to improve New Zealand's ability to tackle money laundering and terrorist financing.

Money laundering and terrorist financing are significant problems both here and worldwide. They allow criminals to hide the proceeds of their illegal activities and to fund serious crimes such as drug offending, organised crime and tax evasion. It's hard to quantify how much money is laundered in New Zealand, but it's been estimated at about $1.5 billion each year.

To combat this issue, many countries around the world have adopted anti-money laundering and countering financing of terrorism (AML/CFT) regimes. These regimes apply to business sectors that domestic and international evidence shows are at high risk of being misused by criminals.

The AML/CFT regime requires businesses to have measures in place that prevent criminals from channelling 'dirty' money through them. The regime also bolsters authorities' ability to detect and investigate serious crimes by following the money trail that such offences generate.

In 2013, Phase One of New Zealand's Anti-Money Laundering and Countering Financing of Terrorism Act came into effect, placing obligations on financial institutions and casinos, and tasking government agencies with overseeing and enforcing the regime and helping businesses to comply with it.

In June 2016, the Prime Minister announced the Government will accelerate Phase Two of the AML/CFT regime, which will extend it to more businesses and professions. The Government intends to introduce a Bill to Parliament later this year, and have it passed by July 2017.

This means:

- many businesses in the following professions will have to put AML/CFT measures in place: lawyers, accountants, real estate agents, conveyancers, some additional parts of the gambling sector and some high-value goods dealers. Dealers of high-value goods that might be affected include auctioneers, bullion dealers, jewellers, precious metal and stone dealers, motor vehicle and boat dealers, antique and art dealers, pawnbrokers and second dealers, and any other business that accepts or provides large amounts of cash.
- there may be minor changes to aspects of the current AML/CFT regime, which will affect professions already subject to it, as well as those it's being extended to.

Your views will help us to determine some of the details of the extended AML/CFT regime, so that we can enhance New Zealand's efforts to detect and deter criminal activity while minimising the impact on businesses.

How to have your say

Along with the rest of this introduction, please read the sections in this consultation paper that are relevant to your sector.

If you're a lawyer, accountant, real estate agent, conveyancer, high-value goods dealer or gambling service provider:

We suggest you read Part 2: New Zealand's approach to addressing money laundering and terrorist financing, which will give you a basic overview of the AML/CFT regime in New Zealand and the proposed changes under Phase Two.

In Part 3: sector-specific issues & questions, you should read the section specific to your profession. For each business sector, we've outlined: the money laundering and terrorist financing (ML/TF) risks you face; case studies of criminal offending; proposals for change and issues to consider; and questions we'd like you to answer.

You should also consider the issues and questions in Part 4: supervision, Part 5: implementation period & costs and Part 6: enhancing the AML/CFT Act.

In particular, Appendix 1: comparison of obligations will help you understand your obligations once Phase Two comes into effect. If you have existing obligations under the Financial Transactions Reporting Act or the Secondhand Dealers and Pawnbrokers Act, it will explain what your additional obligations are likely to be.

If you're a business that's already subject to the AML/CFT regime:

You should consider the issues and questions in Part 6: enhancing the AML/CFT Act.

When you're ready to provide feedback, you can:

- give your feedback online at consultations.justice.govt.nz
- email a submission to aml@justice.govt.nz
- post a written submission to AML/CFT consultation team, Ministry of Justice, SX10088, Wellington, New Zealand

Please provide your views by 5pm, Friday 16 September 2016.

Next steps

Your submissions will help us to develop the legal framework for the enhanced AML/CFT regime.

After the consultation period, we will provide final policy options to the Justice Minister on implementing Phase Two. These options will be informed by your submissions and other evidence. The Justice Minister may then seek Cabinet's agreement to her preferred options. If Cabinet agrees, a Bill will be drafted.

It’s expected the Bill will be introduced to Parliament later this year. You will then have an opportunity to comment on the specific proposals in the Bill when it is considered by a parliamentary Select Committee.

The Government intends to have the Bill passed by July 2017. After that, businesses will need a period of time to prepare for the changes, but the extended Act will come into force as soon as practically feasible.

Part 2: New Zealand's approach to addressing money laundering and terrorist financing

Money laundering is the process criminals use to 'clean' money made from illegal activity to conceal its criminal origins so it looks like it comes from a legitimate source. People and groups who finance terrorism often use similar methods to avoid detection.

A business' reputation and trade can be badly damaged if it is used to launder money.

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

To counter money laundering and financing of terrorism, New Zealand introduced the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

The Act's 3 primary aims are to:

- detect and deter money laundering and financing of terrorism
- contribute to public confidence in New Zealand's financial system, and
- bring New Zealand into line with international AML/CFT standards.

Obligations under the Act

The Act requires specific types of businesses that carry out certain types of transactions to comply with various measures to deter and detect money laundering and financing of terrorism.

The measures greatly reduce the risk of being unwittingly drawn into criminal activity, and are generally regarded as good business practice. They include:

- developing a risk assessment and compliance programme
- undertaking customer due diligence (that is, asking for and verifying customers' identification))
- vetting and training staff
- monitoring accounts
- monitoring compliance and audit, and
- reporting suspicious transactions of customers to the Police financial intelligence unit.

See Appendix 1 for more information about the Act's requirements.

A risk-based approach

New Zealand's approach is risk-based. The two main principles of this approach are:

- AML/CFT efforts should be proportionate to the risks, and
- businesses subject to the Act are well placed to assess the level of risk they face, and to determine how to appropriately manage those risks within the scope of the Act's requirements.

This means that the Act only applies to businesses that undertake activities or provide services that criminals are known to exploit, rather than to all businesses in a particular sector or profession.

It also means that while businesses have specific AML/CFT obligations, they also have some flexibility about where to focus their attention and resources relative to the particular risks they face (for example, due to the type of products and services they offer).

AML/CFT supervision

Businesses that are required to comply with the AML/CFT Act are supervised by an appropriate organisation.

There are currently 3 supervisors – the Reserve Bank of New Zealand, the Financial Markets Authority, and the Department of Internal Affairs. The supervisors build awareness of the AML/CFT requirements and monitor and enforce compliance. They monitor reporting entities by carrying out reviews, on-site visits and other activities.

Penalties for not complying with the Act

Businesses that fail to comply with the Act can face civil and criminal penalties. Sanctions for non-compliance include formal warnings for minor breaches or fines and prison terms for serious breaches. Individuals can be sentenced to up to 2 years in prison and fined up to $300,000; body corporates can be fined up to $5 million.

The Act also gives Police the power to pursue criminal charges where an entity repeatedly fails to comply with AML/CFT obligations, provides false or misleading information, or fails without reasonable excuse to disclose information to Police when requested.

Proposed changes under Phase Two

The Act is intended to cover business activities that pose a high risk of being misused by criminals to conduct financial transactions or purchase assets.

Implementing Phase Two of the AML/CFT regime will have multiple benefits:

- It will reduce the risk of businesses being unwittingly drawn into criminal activity.
- It will improve authorities' ability to detect and investigate serious crimes such as drug offending and tax evasion, by following the money trail that such offences generate.
- Because of its more comprehensive coverage, it will help stop the 'displacement effect' where criminals move their funds to sectors outside of regulated sectors in a bid to avoid detection.

- It will bring New Zealand into line with international best practice and help maintain public and international business confidence in New Zealand's overall financial system. Our regime is informed by the international standards set by the Financial Action Task Force (FATF), an inter-governmental forum which sets global AML/CFT standards. FATF is scheduled to evaluate the effectiveness of New Zealand's regime in the near future, and the results could affect New Zealand's international trade reputation.

Business sectors that will be affected

It's intended that Phase Two of the regime will apply to the following sectors that are currently exempt from it:

- legal profession
- accountants
- real estate and conveyancing
- some high-value goods dealers
- some additional parts of the gambling sector.

In 2010, the FIU conducted a national risk assessment on money laundering and identified that businesses and professions in these sectors are vulnerable to misuse by criminals. The findings are in line with international research.[1] What's more, the FATF requires certain business activities within the Phase Two sectors to be brought within the AML/CFT regime.[2]

However, there's no intention to include all services provided by these sectors within the scope of the Act. Rather, businesses' AML/CFT obligations would be limited to activities that criminals are known to exploit.

Existing regulations & professional standards

Phase Two of the AML/CFT will enhance (and in some cases, replace) businesses' existing obligations to help detect and deter serious crime.

The Financial Transactions Reporting Act 1996 ('the FTR Act') currently requires lawyers, conveyancers, real estate agents and accountants to comply with obligations such as identity verification, record-keeping and reporting suspicious transactions. Some high-value dealers have obligations under the Secondhand Dealers and Pawnbrokers Act 2004.

However, these obligations only apply in limited circumstances and are not as robust as those that apply to reporting entities under the AML/CFT Act. Also, unlike businesses that are currently subject to Phase One, these sectors are not overseen by a supervisory agency that monitors and enforces compliance and provides guidance.

---

[1] *NZ Police Financial Intelligence Unit National Risk Assessment on Money Laundering (2010).* See http://www.police.govt.nz/sites/default/files/publications/fiu-nra-2010-primary-document.pdf

[2] See Appendix 2 to find out more about the FATF recommendations.

Some Phase Two sectors are required to comply with existing professional standards set by their industry bodies. In general, however, these standards differ in nature to those required under the Act.

Proposed changes to enhance the current AML/CFT regime

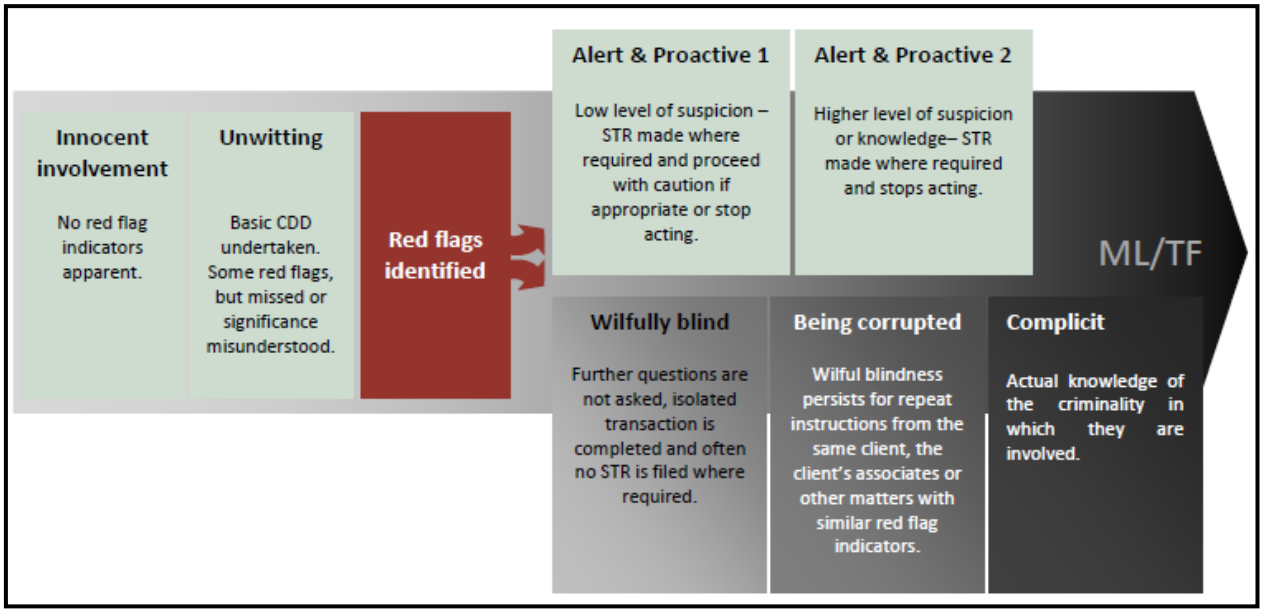
With the introduction of Phase Two, we are also considering opportunities to enhance the operation of the current AML/CFT laws. In Part 6 of this paper, we've identified several issues relating to suspicious transaction reporting, information sharing, customer due diligence and reliance on third parties. We would like your feedback on these issues.

Part 3: sector-specific issues & questions

Lawyers

Risks related to legal services

Lawyers play a vital role in New Zealand society. However, case studies and research here and internationally show that some services provided by legal professionals are attractive to criminals wanting to launder the proceeds of crime and to finance terrorism. While there are some instances of legal professionals being directly involved in money laundering, most lawyers who are exposed to it are not complicit. However, it's recognised internationally that the involvement of legal professionals in the money laundering of their clients is best described as a continuum shown by this diagram:[3]



Note: CDD = customer due diligence; STR = suspicious transaction report

The ML/TF risks associated with legal services include:

- criminals may exploit lawyers as gatekeepers because this can give the impression of respectability and legitimacy, especially in large financial transactions
- criminals may make a deposit or international wire transfer to a lawyer's trust account to send money anonymously

[3] FATF Report: *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (2013).

- criminals may exploit lawyers' conveyancing services when buying or selling property to make their transactions appear legitimate
- criminals may seek lawyers' assistance to establish companies or trusts, which they then use to obscure who really owns or controls the funds and assets (that is, the beneficial owner)
- criminals may seek to use lawyers to conduct multiple transactions that disguise the origin of different sources of funds, which hinders detection and investigation.

Case study 1: using a lawyer's trust account

Two offenders laundered $400,000 cash through a lawyer's trust account in order to buy property. The lawyer didn't conduct due diligence on the offenders or submit a suspicious transaction report. The bank that held the trust account submitted suspicious transaction reports when the lawyer deposited $100,000 cash on 4 occasions. The offenders claimed the cash was held on behalf of their company registered in Gibraltar. They argued the funds were a loan from a company and therefore legitimate.

Source: FIU

Case study 2: using lawyers and real estate agents to make multiple undetected suspicious property transactions

With as much as $500,000 or more generated in 8 months from methamphetamine sales, offenders used criminal proceeds to buy a farm. In a complex series of arrangements that clearly showed an illegitimate transaction, several payments were made to lawyers and real estate agents in the names of at least 3 different people. This prompted bank staff to lodge a series of suspicious transaction reports. Even a courier driver became suspicious about elements of the offenders' operation, causing them to restrict their use of couriers. The lawyers and real estate agents, however, completed the real estate transactions without raising any of these issues.

Source: Ron Pol, AMLassurance.com. Unpublished PhD research. No republication without permission, ©2016.

Issues for consultation

To help ensure we establish a practical regime based on money laundering and terrorist financing risks, please consider the following issues.

Legal services that would be subject to AML/CFT requirements

We seek your views on which activities provided by members of the legal profession should be subject to AML/CFT requirements under Phase Two, and how those requirements should be applied given your business structures and practices.

The AML/CFT requirements are outlined in Appendix 1.

Based on identified risks and international standards, it's proposed that lawyers will be subject to AML/CFT requirements when providing the following services in the ordinary course of business:

- acting as a formation agent of legal persons or arrangements

- arranging for a person to act as a nominee director or nominee shareholder or trustee in relation to legal persons or arrangements
- providing a registered office, a business address, a correspondence address, or an administrative address for a company, a partnership, or any other legal person or arrangement
- managing client funds, accounts, securities or other assets
- preparing for or carrying out real estate transactions on behalf of a customer
- preparing for or carrying out transactions for customers related to creating, operating or managing companies.

This reflects recommendations from the Financial Action Task Force, and would improve New Zealand's ability to detect and deter criminal activity. For example, in some circumstances, lawyers have a fuller picture of their clients' background, circumstances and activities than financial institutions involved in conducting transactions, so a legal professional may be better placed to identify suspicious financial activity.

NOTE: we do not propose including transactions that are solely for the purpose of paying professional fees or invoices.

Also, there is no intention to capture activities of businesses' in-house lawyers, as they do not provide services to external clients.

Legal professional privilege

We also seek your specific feedback about AML/CFT obligations and legal professional privilege.

NOTE: legal professional privilege plays an important role in our legal system and there's no intention to override it in the implementation of Phase Two.

In New Zealand, the main types of legal professional privilege are lawyer/client privilege and litigation privilege. Potential tension between the Act's obligations and legal professional privilege may occur in the following circumstances:

- when a lawyer is required to file an STR under the Act but information relating to the transaction may be privileged, or
- when a sector supervisor requests information from a lawyer under the Act but information relating to the request may be privileged.

This tension is increased by the fact that legal professional privilege is owned by the client and may be difficult for a legal practitioner to determine in some circumstances. As well, changes are being considered to STR requirements under the Act which would extend them to the reporting of suspicious activity (see Part 6).

Currently, a lawyer is required to submit a suspicious transaction report to the NZ Police FIU when:

- there are reasonable grounds to suspect that a client's transaction is suspicious and could be related to criminal activity; and

- legal professional privilege does not apply.

At section 42, the Act states that a communication is privileged if:

a. it is a confidential communication, whether oral or written, passing between—

   (i) a lawyer in his or her professional capacity and another lawyer in that capacity:

   (ii) a lawyer in his or her professional capacity and his or her client:

   (iii) any person described in subparagraph (i) or (ii) and the agent of the other person described in that subparagraph, or between the agents of both the persons described, either directly or indirectly; and

b. it is made or brought into existence for the purpose of obtaining or giving legal advice or assistance; and

c. it is not made or brought into existence for the purpose of committing or furthering the commission of some illegal or wrongful act.

Section 44 of the Act provides protection from criminal, civil and disciplinary proceedings for a person who supplies information about a suspicious transaction if the information is provided in good faith. This approach was adopted to ensure consistency with section 19 of the FTR Act. Currently, lawyers have obligations under the FTR Act to report suspicious transactions in certain circumstances. This doesn't appear to have caused significant practical issues, although the number of STRs are low. However, with the introduction of Phase Two, it's timely to review the protections and consider all practicalities.

In summary, issues to consider include:

- whether the legislative protection of legal professional privilege in the Act (which is consistent with the FTR Act) is sufficient, or whether the current provision is too broad and allows claims of privilege in a wide range of circumstances that aren't appropriate
- whether there's a need to consider addressing AML/CFT issues in practicing rules, or
- whether it would help to publish supervisor or industry guidance on the relationship between the Act's requirements and legal professional privilege. For example, in the UK, the Law Society has published guidance on the interaction between legal privilege and suspicious transaction reporting.[4]

[4] See http://www.lawsociety.org.uk/support-services/advice/practice-notes/aml/legal-professional-privilege/

Questions

1. How should AML/CFT requirements apply to the legal services sector to help ensure the Act addresses the risks specific to it? For example, which business activities should the requirements apply to? At what stage in a business relationship should checks, assessments and suspicious transaction reports be done?
2. Is the existing mechanism that protects legal professional privilege appropriate for responding to money laundering and terrorist financing, and for the legal profession to comply with its expected obligations under the Act? If not, what else is required?

Accountants

Risks related to accounting services

Accountants' specialised skills and services may be attractive to criminals seeking access to the financial system so they can avoid detection or raising red flags. As with the legal profession, case studies and research show some accounting services have been exploited by criminals such as organised crime groups, corrupt public officials and fraudsters. Professional services may also have become more attractive to criminals over the past few years as the financial sector has implemented comprehensive AML/CFT measures.

The ML/FT risks associated with accountancy services include:

- criminals may seek to conduct their financial activity through an accountant to disguise their criminal involvement
- criminals may seek out accountants as gatekeepers to the financial system to give the impression of respectability and legitimacy
- criminals may misuse accountants' trust accounts for deposits or international wire transfers to avoid detection
- criminals may seek the assistance of accountants to establish companies or trusts which they use to obscure who really owns or controls the funds and assets (that is, the beneficial owner).

Case study 1: using accountants to conduct financial activity

A methamphetamine manufacturer and dealer in the Waikato used an accountant to convert cash from his drug dealing into farm land purchases over a number of years. The accountant had 12 accounts with different banks in which he would deposit the cash. The money was then transferred to his accountancy practice and held for his client. The funds were used to purchase farm land in a family trust worth $5 million over 10 years.

Source: FIU

Case study 2: misuse of an accountant's trust account

A criminal investigation identified suspects who had used a trust and the services of an accountant to hide their ownership of criminal funds. The suspects set up a trust and borrowed significant funds to buy their house in the name of the trust. They received about $1.5 million as a commission for consultancy work completed through a company they controlled. The funds were transferred through various accounts to pay for the house. The funds were transferred to an accountant to minimise tax and were then deposited into the mortgage account of the trust.

Source: FIU Typology Report Fourth Quarter 2014/2015 (August 2015)

Issues for consultation

To help ensure we establish a practical regime based on money laundering and terrorist financing risks, please consider the following issues.

Accounting services that would be subject to AML/CFT requirements

We seek your views on which activities provided by members of the accounting profession that should be subject to AML/CFT requirements under Phase Two, and how those requirements should be applied given your business structures and practices.

The AML/CFT requirements are outlined in Appendix 1.

Based on identified risks and international standards, it's proposed that accountants be subject to the Act when providing the following services in the ordinary course of business:

- acting as a formation agent of legal persons or arrangements
- arranging for a person to act as a nominee director or nominee shareholder or trustee in relation to legal persons or arrangements
- providing a registered office, a business address, a correspondence address, or an administrative address for a company, a partnership, or any other legal person or arrangement
- managing client funds, accounts, securities or other assets
- preparing for or carrying out real estate transactions on behalf of a customer
- preparing for or carrying out transactions for a customer related to creating, operating or managing companies.

This reflects recommendations from the Financial Action Task Force, and would improve New Zealand's ability to detect and deter criminal activity. For example, in some circumstances, accountants have a fuller picture of their clients' background, circumstances and activities than financial institutions involved in conducting transactions, so an accountant may be better placed to identify suspicious financial activity.

NOTE: we do not propose including transactions that are solely for the purpose of paying professional fees or invoices.

Also, there is no intention to capture activities of businesses' in-house accountants, as they do not provide services to external clients.

Provision of assurance and advisory services

We also seek your specific feedback about whether certain assurance and advisory services provided by accountants should be subject to AML/CFT requirements. This relates to accountants who provide tax advice, auditing and bookkeeping services as a business.

Different approaches have been taken internationally. For example, in the UK, tax advisors, auditing services and bookkeepers are subject to AML/CFT regulation. This approach recognises that these professionals may, at times, be best placed to detect suspicious activity.

On the other hand, in Canada, AML/CFT regulation of accountants is limited to those who engage in transactions on behalf of clients or give instructions for such transactions. This approach considers that the risk arises in the movement of funds. We seek your views on the appropriate approach for New Zealand given the risks and circumstances.

Questions

1. How should AML/CFT requirements apply to the accounting sector to help ensure the Act addresses the risks specific to it? For example, which business activities should the requirements apply to? At what stage in a business relationship should checks, assessments and suspicious transaction reports be done? Who should be responsible for doing them?
2. Given the level of risk associated with advisory and assurance services (for example, tax advice, bookkeeping and auditing), should these activities be subject to AML/CFT obligations even where the business is not involved in a transaction for their client?

Real estate and conveyancing

Risks related to real estate

The real estate sector has been identified by NZ Police as being vulnerable to money laundering and terrorist financing. The services of real estate agents and conveyancers may be misused by criminals seeking to invest illicit funds in real estate.

The ML/TF risks associated with real estate and conveyancing services include:

- criminals may exploit the services of real estate agents and conveyancers when buying or selling property to appear legitimate
- criminals may seek to provide funds to real estate agents for a deposit on a property and then ask for the funds to be returned before finalising the purchase, which enables them to disguise the origin of the funds
- trans-national criminal groups may seek to invest criminal funds in New Zealand due to its stable economy and strong property market
- given the large size of the transactions, criminals may seek to invest illicit funds in real estate and integrate the funds with savings, to disguise the origin of the funds.

Case study 1: buying real estate using proceeds from the sale of illicit drugs

Several lawyers and real estate agents were involved in facilitating a string of real estate purchases for an offender and associate that were recorded in the names of the associate and relatives of the offender. In relation to the last 2 properties, the offender was an unemployed beneficiary or in prison for drug dealing, making a disproportionate number of purchases that far outstripped his capacity to do so by legitimate means. Although these transactions included a number of red flags that proceeds of crime were being used, none of the 4 real estate agents or 3 lawyers who facilitated the transactions detected them. Another real estate company managed the rental of one of the properties soon after its purchase. That company also facilitated an earlier transaction with similar characteristics involving the same offender, and had briefly employed one of the owners of the property later forfeited under proceeds of crime provisions.

Source: Ron Pol, AMLassurance.com. Unpublished PhD research. No republication without permission, ©2016.

Case study 2: buying real estate for a drug-offending operation

As part of a sustained and commercial drug-offending operation, the offender bought a second property specifically with the intention of cultivating cannabis. The offender told the real estate agent he would not consider houses with indoor electricity meters. He didn't want the electricity company's meter reader to have access inside the house where the intended indoor cannabis crop would be grown. Soon after purchase, the offender arranged for an outside power meter and installed hydroponic equipment for cannabis cultivation, and expanded criminal operations at both properties.

Source: Ron Pol, AMLassurance.com. Unpublished PhD research. No republication without permission, ©2016.

Issues for consultation

To help ensure we establish a practical regime based on money laundering and terrorist financing risks, please consider the following issues.

Real estate-related services that would be subject to AML/CFT requirements

We seek your views on which services provided by real estate agents and conveyancers should be subject to AML/CFT requirements under Phase Two, and how those requirements should be applied given your business structures and practices.

The AML/CFT requirements are outlined in Appendix 1.

Based on identified risks and international standards, it's proposed that real estate agents and conveyancers will be subject to AML/CFT requirements when providing the following services in their ordinary course of business:

- when an agent is engaged, they represent either the purchaser or vendor in the purchase and sale of real estate (both commercial and residential)
- providing conveyancing services as part of the sale or purchase of real estate
- the purchase and sale of properties for development purposes.

NOTE: we do not propose including leasing and property management services provided by real estate agents. This is because the main risks related to the real estate sector are associated with the purchase and sale of property.

When to conduct due diligence on customers

We also seek your specific feedback about the timing of the application of the Act – that is, the point at which a person becomes a customer and you need to conduct customer due diligence on them.

Options include when the real estate agent is involved in a transaction relating to the purchase or sale of real estate (for example, accepting a deposit) or at the point of entering into agreement to act on behalf of the client in a transaction (for example, upon accepting instructions from a client).

Questions

1. How should AML/CFT requirements apply to the real estate and conveyancing sectors to help ensure the Act addresses the risks specific to them? For example, which business activities should the requirements apply to? At what stage in a business relationship should checks, assessments and suspicious transaction reports be done? Who should be responsible for doing them?
2. Should businesses in the real estate sector that engage in property development have obligations under the Act? If yes, in what circumstances?
3. At what stage should a client of a real estate agent become a customer for the purposes of customer due diligence?

High-value goods

Risks related to high-value goods

Buying and selling high-value assets is attractive for criminals because such transactions can avoid interaction with the financial sector. Many such assets may be easily hidden and can be transferred to third parties with limited documentation. In particular, criminals may buy such goods with cash (that is, physical currency) and give them to other parties to avoid detection by financial institutions.

The ML/TF risks associated with high-value goods include:

- In New Zealand, valuable assets such as silver and gold, jewellery and precious stones, cars, boats, artwork and other items have been associated with offenders.
- NZ Police have identified purchases of high-value items, such as precious metals or gems and vehicles, as having a high inherent risk of being misused for ML/TF purposes.
- High-risk red flags include significant or frequent use of cash to purchase valuable commodities and assets, which can then be resold to disguise the origin of illicit funds.
- Criminals may also use cash to buy high-value goods such as jewellery or watches, then travel overseas with them to transfer value while avoiding detection by financial institutions.
- Organised crime groups may use cash to purchase high-value goods then sell them for cash, so they can disguise the origin of the funds and deposit the money into the financial system without raising red flags.
- Criminals use criminal proceeds to buy real estate and luxury goods such as motor vehicles and boats for personal use.

Case study 1: cash purchase of high-value goods

In June 2016, Northland Police seized a record-breaking amount of methamphetamine in Kaitaia – 448 kilos, thought to have an approximate NZ street value of around $448 million. The investigation revealed a cash payment for a $98,000 boat which was used by criminals involved in the importation of significant amounts of methamphetamine found on Ninety Mile beach in June 2016. The investigation is ongoing.

Case study 2: purchase of high-value items with illicit proceeds

In May 2016, 18 people were arrested and charged as part of a large-scale Police operation against the manufacture and supply of methamphetamine. Search warrants were carried out at more than 30 different addresses in Northland, Auckland, Bay of Plenty, Waikato and Canterbury. The Police Asset Recovery Unit seized several high-end vehicles including a highly modified Nissan GTL Skyline vehicle, a Harley Davidson, a Chevrolet Camaro a 2015 Kawasaki motorbike and a boat.

Case study 3: Operation Wigram

In 2013, NZ Police Operation Wigram identified a simple scheme of buying and selling vehicles to launder criminal funds. The offenders used the proceeds of commercial burglaries and methamphetamine dealing to purchase less expensive vehicles in cash. These less expensive vehicles were soon after traded in for a single more expensive vehicle. Although simple, this structure allowed the offenders to structure the effective cash purchase of the final high-value vehicle and establish an origin of funds for the final transaction (the trade-ins).

Source: NZ Police

Issues for consultation

To help ensure we establish a practical regime based on money laundering and terrorist financing risks, please consider the following issues.

Which types of dealers and what cash amounts should the Act apply to?

We seek your views about how to apply the AML/CFT requirements to high-value goods dealers.

In line with international standards, it's proposed that businesses dealing in precious metals and stones above a specific (but yet to be determined) cash threshold will be required to comply with the Act. These obligations are outlined in Appendix 1.

However, given the risks of criminals exploiting other businesses in this sector, it may be appropriate to include dealers in other high-value goods which may accept significant amounts of cash.

We seek your feedback on the following 2 options:

Option 1: dealers in particular high-risk goods

One approach is to require businesses that deal in particular high-risk goods to comply with AML/CFT requirements when selling or buying goods, and when the transaction is made using an amount of cash (physical currency) above an specific threshold.

This may mean the laws would only apply to dealers of precious metals and stones, jewellery, motor vehicles and boats, which are high-value goods that have been identified in criminal cases and proceeds of crime actions.

Under an international standard recommended by the Financial Action Task Force, dealers in precious metals and stones are required to undertake customer identity verification on cash transactions above USD/EUR15,000. However, as the 3 case studies above demonstrate, there may be other high-risk goods in New Zealand.

This approach of focusing on particular high-value goods would address the known risks. However, it may have a displacement effect where criminals buy other high-value goods to avoid detection when using illicit cash.

In considering an appropriate cash threshold, one approach may be to choose the same threshold – $10,000 – as under new prescribed transaction reporting requirements[5] which are yet to come into effect.

Option 2: dealers in all high-value goods

Another option is to extend AML/CFT obligations to all businesses which engage in cash transactions above an applicable threshold.

The scope of this sector could include auctioneers, brokers, bullion dealers, jewellers, precious metal and stone dealers, motor vehicle and boat dealers, antique and art dealers, and any other business that accepts or provides large amounts of cash.

This approach was adopted in the United Kingdom, where any business that accepts or provides cash of EUR15,000 must register with HM Revenue and Customs and implement AML/CFT requirements. In the UK, businesses that don't accept cash above this threshold aren't subject to AML/CFT regulations.

This approach of focusing on all high-value goods would ensure protections are in place for all high-value goods which may be misused by criminals. However, it may be challenging to ensure the wide range of businesses that may be affected by this approach are aware of and put in place AML/CFT requirements.

As with Option 1, in considering an appropriate cash threshold, one approach may be to choose the same threshold – $10,000 – as under new prescribed transaction reporting requirements, which are yet to come into effect.

Questions

1. Should the Act apply to all dealers of high-value goods or just particular ones?
2. What is the appropriate threshold for cash transactions that would trigger AML/CFT customer due diligence and reporting requirements? Please tell us why.

5 Prescribed transactions are international wire transfers of $1,000 or more and domestic physical cash transactions of $10,000 or more. Reporting entities will need to report all transactions that meet the threshold value to Police's Financial Intelligence Unit (FIU).

Gambling sector

Risks related to the gambling sector

Some parts of the gambling sector are known to be at high risk of being misused by criminals for money laundering and terrorist financing. For this reason, the highest-risk part of the sector, casinos, were included under Phase One of the Act.

Now we are considering extending the Act to help ensure there is a 'level playing field' for entities that provide other high-risk services.

The risks associated with the gambling sector include:

- Criminals may use betting accounts to store funds for a short period before transferring them out to justify their income.
- Criminals may use a betting account to 'pool' together funds from multiple sources, which can then be transferred without raising suspicion.
- Criminals may place cash bets at low odds to disguise the origins of the funds and give the impression that the money was made from gambling.
- Intermediaries may place bets on behalf of other people to allow known criminals to anonymously move funds.

Case study: use of a gambling account and purchase of high-value goods

Police Operation Morph related to gang supply of methamphetamine in the Wellington region. Three of the offenders involved, including the principal offender, used purchases of high-value goods to launder the cash proceeds of their drug offending. Paul 'Porky Rimene' Rodgers was captain of the Wellington chapter of the Nomads gang and the principal offender in an enterprise dealing methamphetamine. During 2009–11 Rodgers and his 2 associates, Cole and Laurenson, were receiving benefits, their only sources of income. However, their financial activity didn't match their legitimate income. Rodgers' legitimate benefit income, for example, amounted to $10,000 a year. However, during the period July 2009 to February 2011, $129,000 in cash could be traced through Rodger's accounts and cash spending. $16,000 was also traced through Rodger's online gambling account although he only made one $40 bet.

Rodgers, Cole and Laurenson all made several significant cash purchases between 2009 and 2011 to dispose of cash proceeds of crime. In particular, vehicles were bought and placed in third parties' names to disguise their true ownership. Placement would be achieved by buying the vehicle with a credit card that would then be paid off in structured cash payments.

Source: NZ Police

Issues for consultation

To help ensure we establish a practical regime that reflects the money laundering and terrorist financing risks in your sector, please consider the following issues.

Gambling services that would be subject to AML/CFT requirements

We seek your views on which gambling services should be subject to AML/CFT requirements under Phase Two, and how those requirements should be applied given your business structures and practices.

The AML/CFT requirements are outlined in Appendix 1.

Some parts of the gambling sector are already covered by the AML/CFT regime or have similar (but not as robust) obligations under the Financial Transactions Reporting (FTR) Act. For example, casinos are already covered by the AML/CFT Act, while the New Zealand Racing Board (NZRB) is covered by the FTR Act and must comply with customer identification and verification requirements.

In line with international standards and to create a level playing field, it's proposed that businesses providing other gambling services will have to comply with AML/CFT obligations. For example, a business would have to carry out due diligence on customers who make occasional transactions worth more than a certain amount, or on customers who have accounts with them.

Gambling activities may include the following services provided to customers in the ordinary course of business:

- accepting a bet on behalf of a person
- making a bet on behalf of another person
- providing accounts for the purposes of gambling or betting.

Businesses that might be covered by this proposal include the New Zealand Racing Board, New Zealand Lotteries Commission and junket operators.

As part of this proposal, it's intended that the New Zealand Racing Board and the New Zealand Lotteries Commission should be subject to the AML/CFT regime. The Racing Board was granted an exemption from the obligations of the AML/CFT Act until either Phase Two comes into force or five years from the date of exemption (8 September 2013). Similarly, the Lotteries Commission was granted a ministerial exemption from the Act. These exemptions were granted partly because Cabinet explicitly agreed to include the Board and the Commission in Phase Two of the AML/CFT reforms. It's now appropriate to consider whether these organisations should be fully covered by the Act.

NOTE: It's not intended that pokies in clubs and pubs be included under Phase Two[6] because they are considered a low-risk activity, as the Gambling (Harm Prevention and Minimisation) Regulations 2004[7] set a maximum jackpot limit of $1000.

[6] Class 4 gambling as defined in section 30 of the Gambling Act 2003.

[7] Regulation 6.

Threshold for triggering AML/CFT obligations on occasional cash transactions

We also seek your views on whether AML/CFT obligations should apply to cash transactions worth more than a particular amount that you conduct with customers who you don't have an account relationship with.

Some business activities (such as paying out large winnings or awarding a valuable prize) are at high risk of being abused by criminals, so a threshold is appropriate in those circumstances. For example, casinos currently must meet customer due diligence obligations when they conduct cash transactions of NZD6,000 or more.

Questions

1. How should AML/CFT requirements apply to the gambling sector to help ensure the Act addresses the risks specific to it? For example, which business activities should the requirements apply to? At what stage in a business relationship should checks, assessments and suspicious transaction reports be done? Who should be responsible for doing them?
2. Should there be a threshold that would trigger AML/CFT customer due diligence and reporting requirements for cash transactions related to gambling and betting activities with customers who don't have an account with you? If so, what would be an appropriate threshold? Please tell us why.

Part 4: supervision

To effectively counter money laundering and terrorist financing, business sectors' AML/CFT efforts need appropriate oversight and support.

Agencies known as supervisors play this role. They help ensure businesses implement their AML/CFT requirements, and maintain a 'level playing field' so that businesses are not disadvantaged by competitors not complying with obligations.

The Government is considering how Phase Two businesses should be supervised. Globally, many different AML/CFT supervisory models have been adopted. For example:

- Single supervisor: A single dedicated government agency supervises all AML/CFT sectors and reporting entities. This is the current model in Australia.
- Multi-agency supervision: AML/CFT monitoring and supervision roles and functions are assigned to existing government agencies. The agencies may also be responsible for monitoring businesses' compliance with other requirements, such as prudential regulation. This is our current model; it's also used in the United States.
- Multiple agencies with self-regulatory bodies: AML/CFT supervision is carried out by a single government agency or by many agencies, combined with self-regulation by professional bodies that have been designated as AML/CFT supervisors. This is the current model in the United Kingdom.

New Zealand's multi-agency supervision model

Currently, in New Zealand, under our multi-agency supervision model:

- the Reserve Bank supervises banks, life insurers, and non-bank deposit takers
- the Financial Markets Authority supervises securities, trustee corporations, futures dealers, collective investment schemes, brokers and financial advisers
- the Department of Internal Affairs supervises casinos, money changers, trust and company service providers, and reporting entities not covered by the RBNZ and FMA.

In choosing this model, the Government considered the following objectives, which will also be taken into account when deciding the Phase Two supervisory model:

- compliance with international obligations
- a 'best fit' for New Zealand based on cost benefit and risk analysis (considering the costs on government and business, likely benefits, the level of ML/TF risk, and the likely consequences if we don't comply with international standards)
- consistent regulation and supervision across sectors where feasible, while recognising sector differences

- transparent regulation, rules and sector guidance that are accessible and provide certainty to business and supervisors
- effective and coordinated implementation (including information sharing) to achieve the overall objectives of the framework, and
- regulation and supervision that go no further than necessary to achieve the objectives and which minimise compliance costs to business as much as feasibly possible.

The FATF has produced guidance and undertakes country evaluations to assess the effectiveness of AML/CFT supervision[8]. It has identified six factors that are the basis of an effective AML/CFT supervisory system:

a. Market entry
b. Understanding of ML/TF risks
c. Supervision and monitoring to mitigate ML/TF risks
d. Remedial actions and sanctions
e. Effectiveness of supervisory actions on compliance
f. Promoting a clear understanding of AML/CFT obligations and ML/TF risks

The Ministry will consider the FATF's guidance and relevant recent country evaluations when considering the appropriate AML/CFT supervision model for New Zealand.

Issues for consultation

We seek your feedback about whether the current supervisory model is appropriate for Phase Two of the AML/CFT reforms. We've outlined alternative options and a number of advantages and disadvantages of the different models.

Current model: multi-agency supervision

This is our existing model. The advantage of this approach is that sector supervisors have established structures and methodologies, and are experienced in supervising AML/CFT activities. They also have existing arrangements which support collaboration and consistency across the sectors, such as the National Coordination Committee made up of AML/CFT supervisors, Police's financial intelligence unit and other agencies. The supervisory powers and penalties in the current Act would be extended to Phase Two, further supporting a consistent approach to supervision and enforcement.

However, current sector supervisors may have limited expertise related to some of the sectors to be covered by Phase Two and limited engagement with them. The sectors themselves may also have limited experience in relation to AML/CFT and this model may have a larger impact on Phase Two entities as they may be monitored by both their professional association and their AML/CFT supervisor. Other government or statutory agencies may be better placed to supervise some Phase Two sectors, given their experience working with these sectors.

---

[8] For example, see the FATF Guidance on Effective Supervision and Enforcement (2015) which is available at http://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf

Alternative 1: single supervisor

This model ensures there's a dedicated supervisor that takes a holistic approach to risk-based supervision across different business sectors.

This helps ensure that resources are focused on supervising reporting entities and activities where the risk of money laundering and terrorist financing is greater. This overview of compliance also avoids fragmentation of knowledge between supervisors. This would also mean supervisory activity is consistent and coordinated.

However, this may lead to duplication of effort in some circumstances – for example, while the dedicated agency would supervise AML/CFT requirements, different agencies would oversee other existing regulatory or professional standards requirements. This approach may also affect the supervisor's expertise and knowledge of the respective regulated sectors. In addition, this approach would disrupt the current supervision of Phase One entities.

We recognise that establishing a single supervisor would be resource intensive and involve a lengthy implementation period. Significant establishment costs would be involved in either establishing a new agency or significantly enhancing the capability of an existing sector supervisor.

Alternative 2: multiple agencies with self-regulatory bodies

A combination of existing sector supervisors and self-regulatory bodies could supervise AML/CFT activities. The UK, for example, has 27 AML/CFT supervisors including 22 professional associations in the legal, conveyancing, accounting, and real estate sectors. Reporting entities that don't belong to a professional association or that don't have an association (such as high-value dealers) are supervised by HM Revenue & Customs.

The advantages of this approach include that supervisors have an in-depth understanding of, and a close relationship with, the respective regulated sectors. Professional associations can leverage their regular communications with their sectors to promote and enforce AML/CFT compliance. In addition, professional associations already supervise their members for compliance with professional standards. This leverages existing monitoring activity and may reduce the impact on affected businesses, as it limits the number of bodies monitoring their activities.

However, the UK has acknowledged their large number of supervisors may have led to overlap and inconsistencies in supervision.[9] This issue of consistency will be important in New Zealand's context, although we recognise that we have a relatively small number of self-regulatory bodies in comparison with the UK. The UK's National Risk Assessment also found there's a risk that conflicts of interest could compromise professional body supervision, as these bodies represent and are funded by the firms they supervise. The UK is now considering whether appropriate safeguards should be put in place to address this risk.

This approach could also involve significant change and costs for the professional associations which don't have experience in AML/CFT supervision. Finally, the powers and penalties available to

[9] Available at https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime

professional bodies would need to be reviewed to ensure they're consistent, appropriate and proportionate for AML/CFT supervision, as they're likely to differ between sectors.

Questions

1. Do you think any of our existing sector supervisors (the Reserve Bank, the Financial Markets Authority and the Department of Internal Affairs) are appropriate agencies for the supervision of Phase Two businesses? If not, what other agencies do you think should be considered? Please tell us why.
2. Are there other advantages or disadvantages to the options in addition to those outlined above?

Part 5: implementation period & costs

We recognise that, in order to fully implement AML/CFT requirements, businesses will need time to develop risk assessments and programmes, put in place the associated procedures and controls, and train staff in the new procedures.

Phase One allowed 4 years for full implementation, but we do not expect Phase Two businesses will need the same length of time to prepare. The AML/CFT regime has been operational for 3 years now, and there's a body of knowledge, expertise and guidance available to help businesses get ready.

While the Government made clear in 2008 that the regime would eventually be extended, we expect some Phase Two sectors are more familiar with the requirements or what it means to be regulated than others.

We seek your views about the appropriate implementation period. In particular, we're interested in estimates based on informed analysis of how long it will take businesses to develop and put in place the required AML/CFT measures (see Appendix 1).

We also recognise that meeting AML/CFT obligations requires various resources. We are conducting a separate business compliance cost survey to help us estimate these impacts. The survey has been distributed to several professional bodies that represent businesses and professions affected by Phase Two, and those bodies have distributed the survey to their members.

Questions

1. What is the necessary lead-in period for businesses in your sector to implement measures they will need to put in place to meet their AML/CFT obligations?
2. Where possible, please tell us how you calculated how long it will take to develop and put in place AML/CFT requirements.

Part 6: enhancing the AML/CFT Act

Phase One of the AML/CFT Act came into full force on 30 June 2013. We seek your views on several issues which could be reviewed to enhance the AML/CFT regime and help ensure it remains effective.

Proposal: expanded reporting to the Police financial intelligence unit

We seek your views about whether the suspicious transaction reporting process should be expanded from a transaction-based model to an activity-based model – that is, whether suspicious activity should be reported, not just actual transactions.

The Government Inquiry into Foreign Trust Disclosure Rules conducted by John Shewan (the Shewan Inquiry) made the following recommendation:

> 'The legislation or regulations that govern suspicious transaction reporting to FIU be revised to facilitate the reporting of actual or proposed transactions that have not or will not necessarily go through a New Zealand bank.'

Reporting entities are required to report information about suspicious transactions to the FIU. However, there are some situations when suspicious or unusual activities may not be reported because a transaction does not occur, even though it may provide valuable financial intelligence for detecting crime.

The FATF recommends that if a financial institution suspects or has reasonable grounds to suspect funds are the proceeds of a criminal activity, or are related to financing of terrorists, it should be required by law to report its suspicions as soon as possible to the FIU. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

Expanding the legislation could improve the detection of criminal activities by the FIU receiving broader, better quality and more timely information. We recognise this increase in reporting could lead to higher compliance costs. However, we consider this would be outweighed by the increased transparency of information.

This approach could potentially include activities that don't use the services of a New Zealand financial institution. While this could potentially include cross-border or multi-jurisdictional transactions, we intend reporting requirements would remain restricted to activities connected to New Zealand. This would include activities that haven't yet taken place, businesses not yet formed or incorporated, and accounts or facilities not yet opened.

Question

1. Should the current requirement to report suspicious transactions be expanded to reporting suspicious activities? Please tell us why or why not.

Proposal: information sharing

We seek your views about how existing information sharing arrangements could be enhanced.

Under the Act, the FIU collects suspicious transaction reports submitted by reporting entities, and it will collect additional reports on cross-broader transfers and significant cash transactions when new reporting requirements commence.

This financial intelligence is valuable to assist law enforcement agencies to detect and disrupt criminal activity, and for supervisors to ensure compliance with the Act. The Act allows for information sharing in certain circumstances. With the introduction of new sectors under Phase Two of the Act, some of which have independent regulatory bodies, this is a good time to review current information sharing arrangements to ensure that information is used effectively and appropriately.

There may be benefits in allowing for additional information to be shared between regulators and supervision agencies, where appropriate. This may also reduce compliance costs that may arise for reporting entities through duplication.

The Government Inquiry into Foreign Trust Disclosure Rules by John Shewan (the Shewan Inquiry) highlighted the need to examine strategic intelligence and other legislative arrangements regarding the information sharing between New Zealand's government agencies. Enhancements could potentially be made that could improve the effectiveness of information sharing between government agencies.

Tax evasion

The use of financial intelligence is an effective way of detecting and investigating criminal activity, including tax evasion. Currently, the FIU shares suspicious transaction reports with Inland Revenue in limited circumstances where they consider there's a reasonable suspicion of tax evasion. By expanding the scope of the provisions, Inland Revenue could potentially combine information from broader FIU data with their other intelligence, which may lead to the successful detection and prosecution of people involved in tax evasion.

This kind of information sharing arrangement could lead to more efficient and effective application of the Revenue acts, resulting in more tax being collected. In Australia, there have been major recoveries of taxes due to the Australian Taxation Office having direct access to data from AUSTRAC, the equivalent of New Zealand's FIU.

A revision of the information sharing arrangements would also align New Zealand with the FATF recommendations which state that countries should ensure they have effective information sharing arrangements in place to combat criminal activity. In a report released in September 2015, the OECD also recommended the fullest possible access to suspicious transaction reports be given to tax administrations.[10]

---

[10] OECD: Improving Co-operation between Tax and Anti-Money Laundering Authorities: Access by Tax Administrations to Information Held by Financial Intelligence Units for Criminal and Civil Purposes (September 2015) https://www.oecd.org/ctp/crime/report-improving-cooperation-between-tax-anti-money-laundering-authorities.pdf

Information about customers

Currently, there are limits on supervisors' ability to share information, in particular personal information. We acknowledge that expanding information sharing arrangements may have privacy implications.

Under the provisions of the Privacy Act, the FIU can ask financial institutions for information about account holders. However, under the AML/CFT Act, there's arguably some uncertainty regarding the FIU's ability to ask reporting entities for information about customers. In addition, there may be circumstances not currently permitted under the Act where the FIU could share information with reporting entities to assist in the disruption of criminal activity.

Under section 77, the Act provides protections for reporting entities to engage with the FIU and supervisors. Expanding the information sharing arrangements could include the option to widen this protection so reporting entities can confidently engage with the Commissioner of Police and the FIU.

Information about reporting entities

Government agencies and the FIU cannot inform supervisors if they think a reporting entity may not be meeting its AML/CFT obligations, as this is outside the scope of law enforcement purposes.

This information could be helpful to supervisors when performing risk assessments and determining resourcing allocations. Similarly, relevant supervisors are unable to share information about reporting entities unless it's for law enforcement purposes.

These information gaps can undermine the ability of agencies to determine whether there are reasonable grounds for suspicion to investigate potential criminal activity and take action where warranted.

In summary, the key considerations are:

- **The nature and purpose of the information being shared.** Under the Act, only suspicious transaction reports and related intelligence are able to be shared for enforcement purposes. Expanding the Act to include strategic and regulatory purposes may mean agencies such as Inland Revenue could detect and investigate high-level border offending by transnational organised crime groups. Alternatively, information gathered by other regulatory bodies may be of interest to supervisors to inform the AML/CFT risk profile or other supervisory activity. Reporting entities may have operational information that would be of strategic benefit to other reporting entities or the FIU.
- **Timing and availability of information shared.** Currently the information received from suspicious transaction reports is limited and isolated to that transaction, resulting in a reactive response from enforcement agencies. Widening the availability of information to real time operational information may give relevant agencies the ability to interrogate information across agency systems in real time. This could result in earlier detection and disruption of criminal activities if FIU and other enforcement agencies are able to access and analyse information before a suspicious transaction report is made.

- **Agencies that should be included in information sharing.** The people and agencies that could potentially share AML/CFT information with others are the sector supervisors, industry regulators, intelligence agencies, Inland Revenue, Customs, and other public sector entities. It's also been suggested reporting entities could benefit from sharing information with other reporting entities.

Questions

1. Should industry regulators be able to share AML/CFT-related information with government agencies?
2. Should AML/CFT supervisors be able to share customers' AML/CFT-related personal information with government agencies?
3. What are the appropriate circumstances under which the FIU can share financial intelligence with government agencies (such as the sector supervisors, industry regulators, intelligence agencies, IRD and Customs) and reporting entities? What protections should apply?
4. What restrictions should be placed on information sharing?

Proposal: reliance on third parties

We seek your feedback about whether current third party reliance provisions are appropriate or whether they should be enhanced.

Phase Two will increase the number of small businesses, partnerships and franchise businesses covered by the Act. The Act currently includes 3 provisions for reporting entities to rely on third parties to meet their AML/CFT obligations (though circumstances apply to each one):

- reliance on a member of a designated business group (DBG)
- reliance on other reporting entities or persons in another country
- reliance on agents.

In all circumstances, the reporting entity is ultimately responsible for complying with the Act.

The DBG provision allows reporting entities that are members of the same financial group to (subject to certain conditions) share AML/CFT obligations such as customer due diligence measures and checks, the AML/CFT programme or risk assessment, or filing suspicious transaction reports on another member's behalf.

Question

1. Are the existing provisions that allow reporting entities to rely on third parties to meet their AML/CFT obligations sufficient and appropriate? If not, what changes should be made?

Proposal: trust and company service providers

We seek your views about whether it's appropriate to extend the scope of trust and company service providers covered by the Act.

Money launderers may use legal structures such as trusts and shell companies to hide the beneficial ownership of criminal assets. In addition to New Zealand-based criminals, money launderers based overseas may seek to set up legal structures here to make it more difficult for overseas authorities to trace their funds.

Due to the high risk, trust and company service providers (TCSPs) that provide the following services as the only or principal part of their business must currently comply with the Act:[11]

- acting as a formation agent of legal persons or arrangements
- arranging for a person to act as a nominee director or nominee shareholder or trustee in relation to legal persons or arrangements, and
- providing a registered office, a business address, a correspondence address, or an administrative address for a company, a partnership, or any other legal person or arrangement.

For other types of reporting entities, obligations under the Act generally arise when they provide a service in the ordinary course of business. Accordingly, under Phase Two, we propose to revise the scope of the provision to bring TCSPs into line with the rest of the Act and to ensure their obligations are the same as other professions that provide trust and company services, such as lawyers and accountants.

Question

1. Should the scope of the provision requiring persons providing trust and company services to comply with the AML/CFT Act be extended to activities carried out in the ordinary course of business, rather than just when they're the only or principal part of a business?

Proposal: simplified customer due diligence

We seek your views about whether it's appropriate to expand the types of low-risk institutions that reporting entities are allowed to conduct simplified due diligence on.

The Act currently allows simplified customer due diligence (CDD) to be performed on:

- an entity listed on the NZX
- a government department named in Schedule 1 of the State Sector Act 1988

[11] Regulation 17 Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2011.

- a local authority as defined in section 5 of the Local Government Act 2002
- NZ Police
- the NZ Security Intelligence Service
- any other entity or class of entities specified in regulations.

The AML/CFT (Requirements and Compliance) Regulations 2011 specify that the following entities are customers for the purposes of the Act's simplified due diligence provisions:

a. a person licensed to be a supervisor or statutory supervisor under the Financial Markets Supervisors Act 2011, when the person acts for themselves
b. a trustee corporation, within the meaning of section 2(1) of the Administration Act 1969, when it acts for itself
c. a Crown entity
d. an organisation named in Schedule 4 of the Public Finance Act 1989 or a company named in Schedule 4A of the Public Finance Act 1989
e. a government body that:
    i. corresponds to a government department named in Schedule 1 of the State Sector Act 1988, and
    ii. is located in an overseas jurisdiction with sufficient anti-money laundering and countering financing of terrorism systems and measures in place
f. a registered bank within the meaning of section 2(1) of the Reserve Bank of New Zealand Act 1989
g. a licensed insurer within the meaning of section 6(1) of the Insurance (Prudential Supervision) Act 2010
h. a company whose equity securities are listed on an overseas stock exchange that has sufficient disclosure requirements and is located in a country with sufficient anti-money laundering and countering financing of terrorism systems and measures in place.

The FATF states that where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures. These simplified measures should take into account the nature of the lower risks and should be commensurate with them (for example, the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

We note that currently in New Zealand, State Owned Enterprises (SOEs) aren't included in the simplified CDD provisions. While they're owned by the government, they have been subject to a different risk profile than other government bodies due to their different legal structure and the commercial nature of their operations. .

However, under the State-Owned Enterprises Act 1988, SOEs may represent a lower risk, given that they are owned by the state through the responsible shareholding minister and the Minister of Finance. Therefore, there is limited value in requiring businesses dealing with SOEs to carry out due diligence on the beneficial owner (in this case, the Government), which is currently required in situations when simplified CDD is not permitted.

We also note that currently, simplified due diligence can be carried out on a company listed on the NZX, or on an overseas stock exchange that has sufficient disclosure requirements and is located in a country with sufficient AML/CFT systems and measures in place.

However, when reporting entities are dealing with majority-owned subsidiaries of such companies, the simplified CDD provisions don't apply. Given these subsidiaries face the same ownership and disclosure requirements as their parent companies, it may be appropriate to extend simplified CDD to them. This would mean that due diligence of beneficial owners is not required. We note that the FATF recognises that simplified due diligence may be applied to such majority-owned subsidiaries.

We propose that reporting entities be allowed to conduct simplified customer due diligence on:

- SOEs as defined by Schedule 1 of the State Owned Enterprises Act 1986
- majority-owned subsidiaries of publicly traded entities in New Zealand and in low risk overseas jurisdictions

Questions

1. Should the simplified customer due diligence provisions be extended to the types of low-risk institutions we've proposed above? If not, why?
2. Should we consider extending the provisions to any other institutions?

Appendix 1: comparison of obligations

The Financial Transactions Reporting Act 1996 (the FTR Act) currently requires lawyers, conveyancers, real estate agents, accountants and the New Zealand Racing Board to comply with obligations such as identity verification, record-keeping and reporting suspicious transactions. Also, some high-value dealers have obligations under the Secondhand Dealers and Pawnbrokers Act 2004, or under companies law.

However, these obligations only apply in limited circumstances and are not as robust as those that apply to reporting entities under the AML/CFT Act.

This table compares sectors' current obligations and their proposed obligations under Phase Two. The information for lawyers, conveyancers, accountants, real estate agents and the gambling sector continues on the next page.

Phase Two sectors	Current obligations	When the current obligations apply	Additional obligations (Phase Two)	When the additional obligations will apply
Lawyers, conveyancers, accountants, real estate agents, gambling sector	• Verify the identity of persons paying $10,000 or more in cash or when you suspect the person is trying to launder money through the transaction. • Where the person paying $10,000 or more in cash is conducting a transaction on behalf of someone else, you must verify the identity of the underlying client. • Retain records of documents associated with transactions (including the	• For lawyers and conveyancers, the FTR Act applies only when they receive funds in the course of their business for the purposes of deposit, investment or real estate. • For accountants, the FTR Act applies only when they receive funds in the course of their business for the purposes of deposit or investment. • For real estate agents, the FTR Act applies only when	• Develop and maintain an AML/CFT risk assessment and compliance programme. • Conduct customer due diligence (that is, asking for and verifying customers' identification) in a wider range of circumstances. • Conduct enhanced customer due diligence (such as verifying source of funds) when conducting high-risk transactions. • Proactively monitor accounts	Only businesses that conduct specific types of activities will need to comply. Refer to the relevant section in Part 3 of this consultation document for lists of the proposed activities in your sector. For general information about AML/CFT obligations, visit justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/information-for-businesses/

Phase Two sectors	Current obligations	When the current obligations apply	Additional obligations (Phase Two)	When the additional obligations will apply
(continued from previous page) Lawyers, conveyancers, accountants, real estate agents, gambling sector	nature, amount, currency, date, and parties involved) for not less than 5 years. • Report transactions or proposed transactions to FIU if you reasonably suspect they involve money laundering or proceeds of crime.	they receive funds in the course of their business for the purpose of settling real estate transactions. • In the gambling sector, the FTR Act only applies to the New Zealand Racing Board.	to identify and where appropriate, report suspicious activity to the FIU. • Retain records of documents associated with transactions (including the nature, amount, currency, date, and parties involved) for not less than 5 years. • Report transactions or proposed transactions to the FIU if you reasonably suspect they involve money laundering or the proceeds of crime. • Meet audit and annual reporting requirements. • Be supervised by an appropriate authority.	
High-value goods dealers	• The Secondhand Dealers and Pawnbrokers Act 2004 requires dealers to be licensed and includes obligations to report and hold stolen goods and	As set out in the the Secondhand Dealers and Pawnbrokers Act 2004 and/or companies law.	• High-value goods dealers will have the same obligations as lawyers, conveyancers, accountants, real estate agents, and the gambling sector (see above).	Only businesses that conduct specific types of activities will need to comply. Refer to the relevant section in Part 3 of this consultation

Phase Two sectors	Current obligations	When the current obligations apply	Additional obligations (Phase Two)	When the additional obligations will apply
(continued from previous page) High-value goods dealers	identification and verification requirements for the 'pledger' (ss 51–52). • Dealers registered as companies are also required to retain financial records and submit annual returns.			document for a list of the proposed activities in your sector. For general information about AML/CFT obligations, visit justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/information-for-businesses/

Appendix 2: FATF recommendations

The FATF sets the international standards to combat money laundering and terrorist financing for countries. New Zealand is a member of the FATF and has committed to implementing the FATF Recommendations. The FATF has identified designated non-financial businesses that should be regulated for AML/CFT purposes when providing certain high-risk services. These sectors and related services are set out below.

Designated non-financial businesses and professions: Recommendations 22 and 23[12]

Sector	Relevant services
Lawyers, notaries, other independent legal professionals and accountants	When they prepare for or carry out transactions for their client concerning the following activities: • buying and selling of real estate • managing of client money, securities or other assets • management of bank, savings or securities accounts • organisation of contributions for the creation, operation or management of companies • creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
Real estate agents	When they're involved in transactions for their client concerning the buying and selling of real estate.
Dealers in precious metals and stones	When they engage in any cash transaction with a customer equal to or above USD/EUR15,000.

[12] FATF Recommendations 2012.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Ministry of Justice
Tāhū o te Ture

justice.govt.nz

info@justice.govt.nz

0800 COURTS
0800 268 787

National Office
Justice Centre | 19 Aitken St
SX10088 | Wellington | New Zealand

New Zealand Government

August 2016