AML/CFT Statutory Review

1 — Last update: 17 December 2021

Anti-Money Laundering Consultants Ltd

Table of Contents

1. Glossary

AML/CFT	Anti-money laundering/Countering Financing of Terrorism
Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
AML/CFT_Supervisors	The Department of Internal Affairs, the Financial Markets Authority, and the Reserve Bank of New Zealand, are the entities which regulate reporting entities covered by the AML/CFT Ac
CDD	Customer Due Diligence
DBG	Designated Business Group
DIA	Department of Internal Affairs
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
FMA	The Financial Markets Authority
HVDs	High Value Dealers
IFT	International Funds Transfer
IR	Inland Revenue
ME	Mutual Evaluation (undertaken by the FATF)
ML/TF	Money laundering/terrorist financing
PTR	Prescribed transaction report
RBNZ	The Reserve Bank of New Zealand
SAR	Suspicious activity report
TCSP	Trust and Company Service Provider
TFS	Targeted financial sanctions
UNSCR	United Nations Security Council Resolution
VASPs	Virtual Asset Service Providers

2. About the Author

Thank you for the opportunity for Anti-Money Laundering Consultants Limited (AML Consultants) to comment on the statutory review of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

This submission has been provided by [redacted], Director of AML Consultants.

Relevant Experience & Qualifications

[redacted] has accumulated 20 years experience in the field of financial crime and anti-money laundering.

Employment

- AML/CFT Adviser, Anti-Money Laundering Consultants Limited;
- AML/CFT Adviser, Reserve Bank of New Zealand;
- Deputy Money Laundering Reporting Officer, Bank of New York (London);
- Supervisory Associate and Financial Crime Expert, Financial Services Authority (London);
- Investigator, Enforcement Directorate, Australian Securities & Investments Commission (Sydney);
- Investigator, National Enforcement Unit, Ministry of Economic Development;

In 2002, whilst an investigator with the National Enforcement Unit within the Ministry of Economic Development, she attended a 3-day Financial Crimes and Anti-Money Laundering Course, held at the Royal New Zealand Police College in Wellington.

Between 2003 and 2005 she worked as an investigator within the Enforcement Directorate of the Australian Securities and Investment Commission. During this time she was a member of an investigations team of what was then Australia's largest investigation of cross border money laundering. The investigation came to be known as *Offset Alpine* and involved members of parliament and prominent leaders in the business community.

In 2006 and with a desire to move away from financial crime investigations and into financial crime compliance, she move to the United Kingdom and worked at the Financial Services Authority as an Associate and was appointed Financial Crime Expert for her department. This role required her to prepare strategic initiatives for supervisory associates, including providing training to associates on anti-money laundering and preparing aides and tools to assist in AML supervisory visits. Her employment at the FSA coincided with the enhancement of the FSA's *Advanced Risk Responsive Operating frameWork* (ARROW II). ARROW II had the objective of enabling the FSA to apply a *principles based* regulatory approach for meeting its statutory objectives of identifying and focusing on key risks across the financial services industry. The FSA made use of appropriate regulatory tools to deal with risks or issues arising. Whilst at the FSA, [redacted] gained significant experience of the *'risk based approach'* to regulatory objectives. Her prior background of 13 years of working in roles requiring analytical thinking enables her to easily transfer the application of risk management decision making.

In 2007 she was Assistance Vice President and Deputy Money Laundering Reporting Officer for the Bank of New York, based in London. In this role she assisted in conducting AML/CFT audits for the banks various business units.

In 2008 she was the AML Compliance Manager for the Premium Business Services division of the Commonwealth Bank of Australia. Australia at that time was in the transitional phases of implementing their Anti-Money Laundering and Countering Terrorism Financing Act 2006. [redacted] contributed to the development of the Bank's policies, systems and controls for detecting, mitigating and managing the risk of money laundering. She was responsible for the AML risk assessment framework in the premium business services division and regularly provided guidance and advice to the Bank's AML/CTF Project Team.

In 2009 [redacted] was employed at the Reserve Bank of New Zealand as AML Adviser. During this time [redacted] was a member of the inter-agency working group, established for the development of the AML/CFT Bill. Over a 12-month period she regularly engaged in discussions with the Ministry of Justice and provided advice on the practical applications of the Bill. She also provided input into drafting of official documents, including public consultations. During this year she was elected as New Zealand's representative to attend the Asia Pacific Group Workshop on the Financial Action Task Force Country Risk Methodology. This was a non-residential 5-day training course. As a member of New Zealand's project team for introduction of the AML/CFT Bill, [redacted] was instrumental in designing New Zealand's first AML/CFT sector risk analysis which was distributed by the Department of Internal Affairs in February 2010.

In 2010, [redacted] established Anti-Money Laundering Consultants Limited (AMLC). The objective of AMLC was to assist businesses establish AML/CFT compliance frameworks. AMLC developed regulatory technology, known as AML360. Over the past 7 years, AML360 has been recognised as a leading vendor in innovative AML/CFT technology. In 2019/20, AML360 was successful in 3 of 3 AML RegTech TechSprints hosted by the Australian RegTech Association and AUSTRAC (the Australian Supervisor of AML/CFT). The three *techsprints* involved (1) firm-wide risk assessments, (2) customer due diligence and (3) transaction monitoring.

Presently, [redacted] continues to operate AMLC and manage AML360's technology solutions. The software is used across 7 countries, including banks and small sized businesses.

Qualifications

[redacted]

University Papers

[redacted]

3. Executive Summary

Role of AML/CFT Compliance in New Zealand

AML/CFT compliance has a vital role across the international landscape to detect organised crime linked to money laundering and terrorism financing. By having systems in place that are designed to detect money laundering, there is greater chance of reducing the harm of crimes such as manufacturing and distribution of narcotics, human trafficking and arms trade.

A key component in AML/CFT compliance laws is to develop a collaborate partnership between the business community and government agencies responsible for AML Supervision. This collaborative partnership encourages the business community to have a strong interest in supporting and implementing tools and techniques to detect and report. This allows government to achieve their goals of investigating and prosecuting offences linked to organised crime.

Since 2010 I have worked in the AML/CFT compliance industry in New Zealand and have taken a strong interest in how New Zealand's framework is operating.

There are certain aspects within the framework that are causing significant harm and prevention to its successes and full potential. The greatest harm is arising from the government's lack of commitment to resourcing adequate technological systems. AML Supervisors and the FIU are not operating with technology that allows informed decision making.

Despite the importance of detecting money laundering and terrorism financing, NZ government has not invested in technology that would assist the country to have better outcomes.

As an individual with prior experience of AML Supervision and financial crime investigations, I am aware of the benefits and advantages that adequate technology would provide to AML Supervisors and the FIU. Technology would allow AML Supervisors to perform their functions adequately, with less operational cost, and dedicate resourcing proportionally to the risks faced.

Lack of technology is also failing in the area of suspicious activity reporting. goAML is the system relied on by the Police Commissioner for the private sector to report suspicious activity to the Financial Intelligence Unit (the FIU).

Any reporting system that an AML/CFT framework relies on needs to encourage businesses to be proactive in reporting. goAML does not achieve this. goAML is causing some businesses to spend between 4-8 hours to submit one report. This resourcing commitment is not practical for a small business and therefore the AML/CFT compliance framework is significantly hampered in meeting its objectives.

AML/CFT laws also require businesses to report suspicions arising from **proposed** customers. This means customers who may have set out to establish a business relationship but did not continue. I have received information from businesses that they were prevented from reporting suspicions due to the goAML system providing no flexibility. This related to not having customer data available, such as a date of birth. As the

circumstances did not enable this data to be available, the businesses were unable to report their suspicions.

58 countries use goAML Australia, Canada, the UK and the USA do not use goAML. (Ref: https://www.youtube.com/watch?v=gQaa6YkSs1k)

goAML was a system originally designed for under developed countries who did not have resourcing capability. It was designed for XML Schema reporting for institutions such as banks.

Small businesses do not have resourcing for the XML Schema option. They are forced to report manually. As a database designed for XML Schema, it is strictly structured and may result in the system failing to accept a submission due to a full-stop or a comma being in the wrong place. It is, in simple terms, not fit for purpose. I expand more on the issues of goAML in my submissions responding to consultation questions relating to the FIU.

Risk Based Approach

The AML/CFT framework is designed for principles based monitoring, also known as the ‘risk based approach’. This type of legislation seeks to achieve outcomes, as opposed to setting prescribed rules.

A successful risk based approach to AML/CFT supervision is heavily reliant on capability of data analysis and reporting. To government with oversight responsibility, this is commonly referred to as as Supervisory Technology, or SupTech for short.

New Zealand government has not made any investment in adequate SupTech. As a private individual with modest income, I have successfully worked with software engineers to develop a SupTech model. If I am able to succeed in this regard, why is the NZ government not able to do the same thing?

SupTech has the benefits of allowing AML Supervisors to rapidly analyse risks across their sector. They can do this from sector level or at individual reporting entity level.

Benefits of a risk-based approach to monitoring and assessment

SupTech would provide to AML Supervisors a systematic, risk-based framework for assessing their regulatory objectives. It would enable them to -

- monitor compliance in a cost-effective manner
- target its resources to the highest-priority risks
- respond proactively to changing and emerging risks
- promote sound practices and positive attitudes towards compliance among the regulated sector
- strengthen relationships with the regulated sector.

Minimising Cost Burdens

New Zealand's AML/CFT framework should seek, where possible, to minimise the cost burden to the private sector. A risk-based framework developed with SupTech would allow New Zealand to achieves this.

I have been witnessing a creeping preference of prescriptive measures from the MoJ and AML Supervisors. I believe some of the consultation questions seeking feedback on prescriptive measures is as a result of NZ lacking technology. Some questions tend to suggest a desire to push identification and detection responsibilities from government agencies to the private sector.

An effective AML/CFT risk management framework needs to be intelligence-led and evidence-based. Technology can easily provide these outcomes, however AML Supervisors are using manual processes and are still reliant on spreadsheets.

The use of SupTech would improve sector knowledge of AML Supervisors, improve their level of interaction with their sectors and enhance collaboration and cooperation.

Facilitating compliance requires making processes as simple and convenient as possible, such as submitting suspicious activity reports. New Zealand has not achieved this and the lack of investment in adequate technology is a barrier to New Zealand meeting AML/CFT regulatory objectives.

In the field of financial crime, when government does not investment in adequate resourcing, organised criminals win and the public continue to be the victims of the harm that organised criminals cause.

Resourcing Issues

This statutory review should be focusing on the issues preventing AML/CFT compliance operating efficiently in New Zealand. These can be summarised as -

- Skills and staffing
- Legal and IT support

Investment in these areas would enable AML Supervisors to undertake intelligence-led decision making which would maximise Supervisory effectiveness

Sharing of Information

As the AML/CFT Act was the first piece of legislation that required business to collate an intrusive amount of privacy, the AML/CFT is very strong in protecting such data.

These submissions provide information which indicate breaches from law enforcement agencies is occurring. This is believed to be a systemic problem and has the real risk of significantly harming the reputation of New Zealand's AML/CFT framework.

I provide more information on this under the chapter *'Information Sharing'.*

NZ has no dedicated anti-corruption agency

Corruption and bribery are closely connected to money laundering.

The AML/CFT Act is a powerful piece of legislation. There are no limits to what personal information a business ma seek from its customers. This can include passports, driver licenses, bank statements, source of wealth, copies of trusts and value of assets. This type of data in the wrong hands can cause significant harm to an individual.

I strongly advocate it is well overdue for New Zealand to establish an anti-corruption agency. An anti-corruption agency should be considered a further tool for New Zealand to reduce the risk of money laundering and enhance its governance controls to reduce crime.

Time Restraints

Time restraints have prevented me from responding to all consultation questions.

If there is an opportunity to present to the Select Committee, I would appreciate the chance to do so.

4. Institutional arrangements and stewardship

Consultation Document

This section focuses on the fundamental aspects of our AML/CFT regime and offers an opportunity to reconsider the principles upon which the regime was based when it was developed in 2009. It is important that purposes, structure, roles, and responsibilities are still appropriate and that they help to ensure the regime remains fit-for-purpose in the fight against money laundering and terrorism financing.

Consultation Guiding Questions

• Are the foundations of our AML/CFT regime correct? Does the regime have the correct purposes for what it is aiming to achieve, or do the purposes need to be updated?

• Are the right agencies involved, and do they have the appropriate powers? Should the Act better enable the private sector to be a partner in the fight against serious and organised crime?

• Does the Act strike the right balance between allowing a risk-based approach and ensuring that obligations are clear for businesses?

4.1. Purpose of the AML/CFT Act

Statutory Review Consultation Document

The purpose of the AML/CFT Act (as set out in section 3) is to:

- detect and deter money laundering and terrorism financing; and
- maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations by the Financial Action Task Force; and
- contribute to public confidence in the financial system.

These purposes were set when the Act was originally introduced in 2009, however the landscape – both domestically and internationally – has evolved since. It is timely to consider whether the purposes of the Act are still appropriate and whether there are any changes that should be made.

Statutory Review Summary Document

We want to make sure what the Act is trying to do is still relevant to New Zealand and ask questions about the purpose and goals of the Act. And the Act itself requires a review. The Act currently has three goals: putting off others from laundering money and financing terrorism and spotting it when it happens, complying with our international obligations, and making sure the public is confident about our businesses operating lawfully.

We set the goals for the Act in 2009, but a lot has changed since. We want to hear views about whether we need to update the goals of the Act. One potential change we want to explore is whether the Act should have the goal of actively stopping money laundering and terrorism financing, instead of putting people off from doing this.

4.1.1. Actively Preventing ML/FT

Consultation Questions

- Should a purpose of the Act be that it seeks to actively prevent money laundering and terrorism financing, rather than simply deterring or detecting it?

- If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there needs to be any additional or updated obligations for businesses?

Response

The current purpose of the AML/CFT Act obligates a regulated business to 'detect' and 'deter' (Section 3).

- *Deterring* is met by the business establishing policies, procedures and controls, which include the need for a reporting entity to independently verify the customer and confirm the nature and purpose of the customer's business relationship.

- *Detecting* is achieved through obligations of ongoing monitoring which includes keeping client information up-to-date, assessing the risk profile of the customer and reviewing the customer's account activity.

For a business to *actively stop* an act of ML/FT would likely require the regulated entity to refuse the activity or seek consent from the FIU before they can continue with the customer's activity. A great proportion of suspicious reporting is known to be mostly defensive reporting and not based on informed decision making. Any laws obligating a business to deny the right of a customer to transact, would be excessively punitive to that individual.

A purpose of the AML/CFT Act includes, *"contribute to public confidence in the financial system"*. It would be difficult for the public to have confidence in New Zealand's financial system when the public (a customer) may have their transaction or activity stopped, without notification and without receiving informed reasoning.

Severe financial harm may result from denying a customer the right to transact, such as a customer failing to meet settlement terms of a real estate transaction because the mortgage lender held a suspicion. The results would be disproportionate to the circumstances.

Under the present law the business community works in partnership with the FIU by detecting and reporting suspicions to the FIU. The FIU may then use that information to support or commence a criminal investigation. Whether the alert results in stopping ML/FT can only reasonably be measured following law enforcement action, including seizure of criminal assets.

In summary, the inclusion of 'stopping' or 'to actively stop' ML/FT should not be a purpose of the AML/CFT Act:

- It is the role of the FIU to stop ML/FT – not the business community.
- It is difficult to measure if criminal activity has been stopped.
- Requiring the FIU to consent to a transaction proceeding will become incredibly burdensome to the FIU, which is already struggling with resourcing commitments.
- There is real risk that stopping a transaction or activity proceeding would result in unjustified actions against innocent individuals.
- Stopping a transaction such as settlements for real estate, securities or investments is likely to result in significant financial harm to the impacted parties.
- Regulated entities are more likely to face legal repercussions from disgruntled customers who challenge their decision making. This would have a material impact on the business and increase the costs and burden of AML/CFT compliance.
- Penalising a private individual, business or corporate entity on the basis of a suspicion rather than fact is regulatory overreach.
- Enacting this power to a reporting entity will more likely erode public confidence in the financial system and be counter-intuitive to the AML/CFT Act's objectives.
- A reporting entity already has the ability to refuse a customer's business and to close the account. The ability to refuse business based on discretion would be more effective than a refusal of business based on a statutory requirement.
- Enforcing a regulated entity to cease business with a customer is more likely to tip-off the customer.

4.1.2. Proliferation Financing

Consultation Questions

- Should a purpose of the Act be that it also seeks to counter the financing of proliferation of weapons of mass destruction? Why or why not?

Response

Pursuant to the United Nations Security Council Resolution 1540 (UNSCR 1540), issued in 2004, New Zealand is already obligated to take measures in order to prevent the proliferation of nuclear, chemical or biological weapons, including proliferation financing. If the MoJ is wishing to strengthen its obligations in this area, it should focus on the ability for New Zealand to issue autonomous sanctions.

In the context of New Zealand problem of international organised criminal groups, reporting entities can readily acknowledge the need for efforts to detect money laundering. Reporting entities are less convinced that financing of terrorism is a problem in New Zealand and introducing a new arm of the AML/CFT Act, namely detection of proliferation financing, is likely to cause reporting entities to disconnect from the AML/CFT Act.

An alternative is to include the offence of *proliferation financing* in the Terrorism Suppression Act which would allow the purpose of the AML/CFT Act to remain unchanged.

Summary

- There are other measures available to the MoJ to strengthen its ability to comply with UNSCR 1540, without needing to change the purpose of the AML/CFT Act.

- Amending the AML/CFT Act to include proliferation financing has a high likelihood of causing discord across the business community.

- Amending the AML/CFT Act to include proliferation financing is likely to negatively impact on the AML/CFT Act as a whole in that businesses may perceive the AML/CFT Act has a purpose in other countries but not in New Zealand.

- Introduction of proliferation financing within the AML/CFT Act would not capture the higher risk industry exposed to proliferation financing such as freight carriers and ship lease companies.

4.1.3. Targetted Financial Sanctions

Consultation Questions

- Should the Act support the implementation of terrorism and proliferation financing targeted financial sanctions, required under the Terrorism Suppression Act 2002 and United Nations Act 1946? Why or why not?

Response

- The AML/CFT Act needs to have some reference for reporting entities to comply with sanctions as issued under the Terrorism Suppression Act.

- With the exception of banks, businesses are not familiar with sanctions. AML Supervisors need to increase their guidance material on what sanctions are, why they exist and what an entity is required to do upon identifying a potential customer or a customer’s 3rd party as a sanctioned individual and/or entity.

- Without the AML/CFT Act explicitly requiring a reporting entity to consider designated entities as contained under the Terrorism Suppression Act, the AML/CFT Act is considerably weakened in its ability to detect and deter terrorism financing.

4.2. Risk Based Approach to Regulation

Statutory Review Consultation Document

At its core, any AML/CFT regime should be risk-based: there should be an assessment of money laundering and terrorism financing at the national, sectoral, and business level, and regulation should be focused on mitigating any risks identified. A risk-based approach should also ensure that an AML/CFT regime is flexible and adapts to changes in risks, and that resources are allocated efficiently and in proportion to levels of risk.

Statutory Review Summary Document

A key idea in our regime is that we should take a “risk-based approach”. In other words, the things that businesses do to protect themselves should be in line with the chance or risk of money laundering or terrorism financing happening. However, our Act does not fully follow this approach: in some places we set strict rules that all businesses have to follow in an effort to provide more certainty. We want to check that we have the right balance between a risk-based approach and providing businesses with certainty about what they need to do.

4.2.1. Understanding our risks

Consultation Questions

- What could be improved about New Zealand's framework for sharing information to manage risks?
- Are the requirements in section 58 still appropriate? How could the government provide risk information to businesses so that it is more relevant and easily understood?

Response

How can NZ improve its framework for sharing information and managing risks?

Thematic and targeted reviews by AML Supervisors should play an important role in NZ's AML/CFT framework.

Using targeted thematic reviews as a regulatory tool would assist to identify systemic risks at both sector and reporting entity level and reduce the probability of failure. Targeted reviews should focus on high risk areas such as risk management, ongoing monitoring and Know Your Customer.

Are the requirements of section 58 still appropriate?

There will always be a need to ensure a reporting entity understands the ML/FT risks that their business faces. If a ML/FT risk assessment was not mandatory, it is likely business owners, based on lack of knowledge, would question the relevancy of ML/FT compliance laws and fail to operate with the appropriate level of controls to detect and deter ML/FT.

Section 58(1) places the onus upon the reporting entity to understand their risks and by doing so, take responsibility and play their part in keeping New Zealand a safe place to conduct business.

Section 58(2) guides the reporting entity on the primary areas where risk arises.

Section 58(3) requires the risk assessment to be in writing. This allows the business to demonstrate their level of knowledge and provides an AML Supervisor with information about the business that an AML Supervisor may not otherwise have. If there was not the need for the risk assessment to be recorded in writing, it is likely business owners, managers and executives of the business would fail to make efforts to understand and identify the risks their business must manage.

Risk information from government

The AML Supervisors have provided reasonable information to assist reporting entities understand the elements within a business that increases ML/FT risk. However, what needs to be recognised is the majority of reporting entities regulated under the AML/CFT Act are small businesses. This in particular is relevant to the Department of Internal Affairs (the DIA), where 60% of reporting entities supervised by the DIA fall into this category (advised by the DIA at an auditors' forum in June 2021).

ML/FT risks mean different things to different people. In the situation of 10 reporting entities facing the same or similar ML/FT risks, the AML Supervisor can very well receive 10 very different outcomes. To overcome this problem, AML Supervisors could provide reporting entities the option of using a standardised methodology which is sector focused. Should an option of a standardised approach be available it would have the benefit of:

- Providing the reporting entity with a level of assurance that they are meeting regulatory expectation;
- Reducing compliance costs to the reporting entity;
- Enabling the AML Supervisor to ensure key criteria is being captured, which otherwise might be overlooked by a reporting entity;
- Provide both the reporting entity and the AML Supervisor with reliable data for informed decision making on the types of policy, procedures and controls that should be in place, based on the risks identified;
- Enable the AML Supervisor to have a consistency of data and be in a better position to conduct comparative analysis across individual sectors for identifying those reporting entities that present the greater risk to their regulatory objectives.
- Reduce human resourcing commitments for AML Supervisors.

One size does not fit all

Problems I have seen with the FMA and DIA AML Supervision is the expectation that the outcome of a reporting entity's inherent risks must match the Supervisor's sector risk analysis. This is not the correct approach and fails to recognise that the risk based approach is not a 'one size fits all' outcome.

When reporting entities operate in the same sector but there are material differences in their core business operations, the risk outcomes should reflect those material differences. To exaggerate the issues, I have illustrated this in the table below:

Reporting Entity A	Reporting Entity B
Sector: Money Remittance	Sector: Money Remittance
Branches: 5 (3 offshore)	Branches: 1 (domestic)
Employees: 8	Employees: 4
Part-time Compliance Officer	Full-time Compliance Officer
Products & Services: 4	Products & Services: 1
Volume of Trade: 1,000,000	Volume of Trade: 2,000
Value of Trade: $225M	Value of Trade: $70,000
Customers: 1,000	Customers: 100
Method of delivery: 100% online	Method of delivery: 100% face-to-face
Geographies: High Risk 7	Geographies: High Risk 0

Based on the above hypothetical corporate data, an AML Supervisor should expect the risk assessment for Reporting Entity A to result in a higher inherent risk than Reporting Entity B. If Reporting Entity B's risk factors result in having a lower risk rating than an AML Supervisor's sector risk survey, this does not mean that Reporting Entity B has not met requirements of section 58 of the AML/CFT Act. This is because Section 58 has the expectation that a risk assessment *reasonably* inform –

*"…. a reporting entity must first undertake an assessment of the risk of money laundering and the financing of terrorism (a risk assessment) that it may **reasonably expect** to face in the course of its business* (the emphasis is mine).

4.2.2. Balancing Prescription with Risk Based Obligations

Consultation Questions

- What is the right balance between prescriptive regulation compared with the risk-based approach? Does the Act currently achieve that balance, or is more (or less) prescription required?
- Do some obligations require the government to set minimum standards? How could this be done? What role should guidance play in providing further clarity?
- Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?

Response

Prescriptive rules versus risk-based principles

Risk-based regulations specify required outcomes and objectives. They encourage reporting entities to implement compliance strategies, proportionate to their nature, size and complexity. This allows small businesses to manage compliance costs and operate on a level playing field.

Prescriptive based legislation has the risk of increasing compliance costs to the extent that it may no longer be viable for a small business to operate. This would defeat the purpose of New Zealand's AML/CFT law in that it seeks to – *'contribute to public confidence in the financial system'* (section 3 AML/CFT Act).

AML/CFT laws are ultimately designed to achieve co-operation between the business community and law enforcement bodies. It is therefore more appropriate that AML/CFT laws focus on government setting principles and outcomes, rather than focusing on technical breaches and enforcement action. AML/CFT laws that are overly prescriptive would not harmonise the business and government partnership that AML/CFT compliance seeks to achieve.

However, to enable outputs from reporting entities to align with statutory objectives, it would be reasonable to expect a minimum level of prescription. Prescription also provides certainty on what must be done in order to achieve regulatory expectation.

New Zealand's AML/CFT Act, in my opinion, has got the balance right in setting out when a reporting entity must meet prescriptive requirements.

Setting minimum standards

Minimum standards are appropriate when the standard ensures a regulatory outcome is achieved. Minimum standards should apply to those areas of the AML/CFT Act that are of primary importance to the overall effectiveness of an AML/CFT framework. Examples include section 58(2) where it sets out those areas of a

business that a reporting entity must have regard to when conducting a risk assessment.

Other examples of where the AML/CFT Act uses the right level of prescribed rules include: (a) the criteria that must be included in an AML/CFT Programme (section 57), (b) minimum requirements that must be achieved before a customer is considered to be reliably verified, (c) circumstances of when a customer must be subject to enhanced due diligence (section 22) and (d) the type of transaction data that must be retained to enable reconstruction of that transaction (section 49). These are examples of where setting prescriptive requirements are proportionate to the objectives that the AML/CFT Act seeks to achieve.

Material from AML Supervisors in the form of Codes of Practice and Guidelines should continue to be used for the purpose of providing clarity to regulatory expectation and setting 'safe harbour' standards.

Ensuring regulatory obligations are proportionate to risk exposure

AML Supervisors should expect all reporting entities to be operating with adequate compliance tools to detect when a customer compliance activity is unusual or suspicious. This regulatory obligation is set out in section 31 (ongoing customer due diligence and account monitoring).

The higher the risk exposure and complexity of the business, the more sophisticated its systems and controls should be for meeting obligations of monitoring and reporting suspicious activity.

If a reporting entity is not operating with effective ongoing customer due diligence controls, AML/CFT objectives cannot be met.

AML Supervisors could do more in this area to ensure the balance is right between regulatory obligations and risk exposure of reporting entities. By requiring higher risk businesses to separately report on their policies, procedures and controls for meeting obligations of ongoing monitoring, AML Supervisors will be in a better position to measure with a reporting entity is meeting regulatory expectation.

I provide further comment on this topic under the chapter *'Powers and Functions of AML/CFT Agencies'*.

4.2.3. Capacity of Smaller and Larger Reporting Entities

Consultation Questions

- Does the Act appropriately reflect the size and capacity of the businesses within the AML/CFT regime? Why or why not?

- Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to and the size of the business? If so, what?

Response

The AML/CFT Act does not distinguish between the size or capacity of a reporting entity. This, in my view, is the correct approach.

A small sized reporting entity can cause the same level of harm as a large institution. Due to limited capacity in systems and resourcing of small institutions, they in fact operate with increased regulatory exposure. Further, criminals are more likely to shop for a small business with knowledge that AML/CFT policies and systems are likely to be less sophisticated and therefore easier to set-up a business relationship and facilitate dirty money.

I have seen circumstances of small entities that are high risk operating without any risk assessment or programme in place. Despite this information being disclosed to the DIA in annual regulatory reporting, no follow-up action was taken by the AML Supervisor. This indicates systems of regulatory reporting are not operating effectively.

Ideally regulatory reporting should automatically alert AML Supervisors to a regulatory breach and result in an automated notification to the reporting entity, informing of the beach and the action to take. This is the benefit of SupTech. It allows a compliance framework to operate with greater efficiency.

As the legislation is already established under principles based laws, addressing aspects of risks and proportionality of size of business is already catered to.

Summary

- The expectation to meet regulatory objectives should be equal across reporting entities, regardless of size or capacity of business.

- It would be the wrong approach for AML Supervisors to focus more on large size institutions and be less involved with small entities. Greater harm can result from small entities due to lack of governance, resourcing and systems.

- Small entities require more guidance and oversight in comparison to a large institution.

- If a large institution operates with risk management committees, dedicated AML compliance staff and systems designed to automatically detect and report, the larger institution presents less threat to statutory objectives.

- AML Supervisors should be using regulatory data to identify those entities most likely to be breaching compliance obligations, based on capacity restraints. If the small entity is also operating in a high risk sector, regulatory oversight should be actioned. Regulatory oversight should include education and advice. This would be the correct application of risk-based supervision.

4.3. Mitigating Unintended Consequences

Statutory Review Consultation Document

While the AML/CFT regime aims to prevent harm, misapplying AML/CFT measures can have serious negative and unintended effects which should be avoided or mitigated. These include making it harder for legitimate non-profit organisations to operate, closing accounts of risky customers or businesses, and excluding people from the formal financial system. This issue is not unique to New Zealand: internationally, the FATF has recognised a number of areas where implementing AML/CFT has inadvertently harmed others.

Statutory Review Summary Document

While the Act aims to keep New Zealand safe, sometimes the Act can make it difficult for people going about their daily lives. We know that the Act has made it harder for some people to open bank accounts. This can make it hard for people to take part in society and can also make it hard for people to send money overseas for valid reasons.

We want to understand how the Act may be causing challenges for people and businesses. We are also interested in knowing if there are any other unintended consequences and how we can fix the challenges we have identified.

4.3.1. Derisking

Consultation Questions

- Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?

- How could the regime better protect the need for people to access banking services to properly participate in society?

- Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them?

Response

In New Zealand, de-risking has primarily impacted on money transfer services, also known as money remittance. The AML/CFT regime has failed to prevent blanket de-risking which has resulted in a high risk sector, now operating outside of the regulated market. This has negatively impacted on New Zealand's ability to meet the purpose of the legislation as set out in section 3.

Banking facilities are an essential service for businesses to operate. Denial of an essential service should be based on informed decision making. Blanket de-risking therefore fails to meet the principles of the AML/CFT Act. Decisions to refuse a reporting entity a business relationship have not been made on a case-by-case, risk based approach. Banks have made their decisions without informed judgements on the real risks presented by individual reporting entities. Banks have instead focused on known inherent sector risks and prejudged all businesses operating in that sector. Financial exclusion impacts on the ability for a fair and orderly market to operate.

Non-bank service providers traditionally provide lower fees than banks. De-risking has resulted in this service sector being pushed out of the market. This has restricted market competition and resulted in increased transaction fees for the transfer of funds across borders.

The consequences of de-risking has resulted in economic and personal harm:

- Business have been forced to close;
- Employees and business owners have lost income and faced financial hardship;
- Money remittance services that have continued operating, albeit without a bank account, have been forced to stock pile cash, increasing their exposure to robbery and personal harm;
- Money remittance services are now operating outside of the regulated market;
- Families reliant on receipt of funds from their members living abroad, have suffered financial hardship.

The harm that has occurred cannot be undone. The focus now needs to shift on how to prevent the ongoing consequences. Some suggestions are provided below:

- To ensure a fair and orderly market, banks should be obligated to disclose their decision-making principles and processes to their AML/CFT Supervisor (the RBNZ). This would work towards ensuring banks are following a risk-based approach and that their decision making is fair and proper.

- Banks who have been found to refuse banking facilities without merit, should be financially penalised.

- The DIA should undertake a thematic review of the money remittance sector in order to understand the real risks that this industry presents in New Zealand.

- The RBNZ should undertake a thematic review of the banking sector to understand the real risks that the sector is concerned about.

4.4. The Role of the Private Sector

Statutory Review Consultation Document

Effective partnership between the public sector and the private sector is essential to combat financial crime. However, New Zealand will always be vulnerable to money laundering and terrorism financing if only some businesses are properly addressing their financial crime risks while others are not. Increasingly, businesses in other countries are taking an approach of “not in my country” rather than “not in my firm” and are actively cooperating to ensure that financial crime and dirty money has no place in their sector.

We want to explore whether the Act should support a “not in my country” approach being taken in New Zealand and how the Act could support a stronger partnership between the private sector and government. We have strong but limited examples of a partnership approach being taken, such as the “Financial Crime Prevention Network,” a public-private partnership between New Zealand Police, New Zealand Customs Service, and several banks, which was established to enable better collaboration on investigating financial crimes.

4.4.1. Partnering in the Fight against Financial Crime

Consultation Questions

- Can the Act do more to enable private sector collaboration and coordination, and if so, what?
- What do you see as the ideal future for public and private sector cooperation? Are there any barriers that prevent that future from being realised and if so, what are they?
- Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime?

Response

Auditors and Consultants

AML/CFT auditors and consultants play an important role in New Zealand's AML/CFT regime. Auditors provide a third line of defence for reporting entities and audit reports are relied on by Supervisors to direct their supervisory approach.

Despite the important role that auditors and consultants provide to the AML/CFT regime, the AML/CFT Act does not explicitly acknowledge the value that auditors and consultants (as AML experts) provide to the regime. There is no obligation upon AML Supervisors to collaborate and co-ordinate with that division of the private sector.

To enhance New Zealand's AML/CFT regime, the AML/CFT Act or regulations should obligate Supervisors and/or, the Co-ordination Committee, to collaborate with auditors. This would enable consultants and auditors to operate under a formalised communication channel which can be utilised when it is necessary to raise concerns or queries.

Obligating AML Supervisors to co-ordinate with the auditing sector will result in better outcomes for reporting entities and the supervisory framework. It would also improve the quality, standards and outcome of audits and ensure a level of consistently across the auditing sector.

4.4.2. Helping to Ensure the System Works Effectively

Consultation Question

- Should the Act require a mechanism to enable feedback about the operation and performance of the Act on an ongoing basis? If so, what is the mechanism and how could it work?

Response

The AML/CFT Co-ordination Committee has a pivotal role for ensuring the AML/CFT regime is operating as intended. The functions of the Co-ordination Committee are detailed in section 152 and include:

- *facilitate good practice and consistent approaches to AML/CFT supervision between the AML/CFT supervisors and the Commissioner;*
- *facilitate the production and dissemination of information on the risks of money-laundering offences and the financing of terrorism in order to give advice and make decisions on AML/CFT requirements and the risk-based implementation of those requirements;*
- *provide a forum for examining any operational or policy issues that have implications for the effectiveness or efficiency of the AML/CFT regulatory system.*

Though section 150(2) prevents any person working in the private sector from being a member of the Co-ordination Committee, it does not prevent any member from the private sector from making representation to the Co-ordination Committee, whether in person or in writing. Nor is there any part of the Act that stipulates considerations and determinations of the Co-ordination Committee must remain confidential and not for disclosure to the private sector.

If the Co-ordination Committee is closed to representations from private industry stakeholders, such as reporting entities, auditors and consultants, it is difficult to envisage how the Co-ordination Committee can adequately perform its functions. In fact, prohibiting the representation of private industry stakeholders would make it impossible for the Co-ordination Committee to perform its regulatory obligations, set out at Section 152(f) to – *“provide a forum for examining any operational or policy issues that have implications for the effectiveness or efficiency of the AML/CFT regulatory system”*.

Summary

- Through the appointment of a Co-ordination Committee, the AML/CFT Act already has a mechanism to enable feedback about the operation and performance of the Act.

- The issues that the statutory review should address is that the Co-ordination Committee has not been operating effectively in practice.

- In attempting to ensure that the AML/CFT regime is working effectively, on an ongoing basis, the Co-ordination Committee should be obligated to meet regularly (quarterly or six-monthly).

- Operating in secrecy does not promote trust from the private sector. Where matters are not considered confidential or sensitive, the Co-ordination Committee should be obligated to provide written reports to the private sector, detailing their considerations and determinations.

- The above criteria acts to ensure the Co-ordination Committee does not operate on a bias in favour of government agencies.

4.5. Powers and Functions of AML/CFT Agencies

Statutory Review Consultation Document

The administration, application, and enforcement of the Act and regime involves six agencies:

- Ministry of Justice is responsible for administration of the Act. The role of the Ministry is set out in section 149
- Department of Internal Affairs, Financial Markets Authority, and Reserve Bank of New Zealand are designated as AML/CFT supervisors. The functions and powers of the supervisors are set out in sections 131 and 132.
- New Zealand Police is responsible for a variety of financial intelligence functions (set out in section 142) and powers (set out in section 143), including receiving SARs and disseminating financial intelligence products.
- New Zealand Customs Service does not explicitly have its functions outlined in the Act, but it is responsible for managing movements of cash across New Zealand’s borders.

Powers of the Financial Intelligence Unit

We have identified some gaps in the powers of the FIU and Commissioner of Police, and filling these gaps could enhance the operation of the regime overall.

Allowing information to be requested from other businesses
The FIU is unable to request information from businesses which are not reporting entities, but which may have relevant information that allows an overall picture to be formed about what is happening. For example, travel agents or airlines may have information relevant to understanding potential terrorism financing threats, which the FIU may need to obtain in time-sensitive situations.

4.5.1. Powers of the Financial Intelligence Unit

Consultation Questions

- Should the FIU be able to request information from businesses which are not reporting entities in certain circumstances (e.g. requesting information from travel agents or airlines relevant to analysing terrorism financing)? Why or why not?

- If the FIU had this power, under what circumstances should it be able to be used? Should there be any constraints on using the power?

Response

This consultation query seeks ability for the FIU (an arm of the NZ Police) to use the guise of the AML/CFT Act, to obtain information, without warrant, from a business that has no regulatory obligations under the AML/CFT Act.

The FIU is not an investigative arm of the NZ Police. The intended function of an FIU is focused on receipt of data, analysis of the data and should an investigation be warranted, the FIU is obligated to disseminate that information to a law enforcement agency (section 142). There are no explicit or implicit powers for the FIU to make enquiries or investigate matters contained in a suspicious activity report.

New Zealand already operates with statutory powers that enable law enforcement agencies to obtain information from third parties, such as travel agencies or airlines. These existing powers require that the investigation body applies in writing for a search warrant and that the threshold must meet “reasonable belief”, not “reasonable suspicion”. This point is relevant as matters reported to the FIU are formed on the basis of ‘suspicion’, not ‘belief’.

Autonomy and Accountability

The core functions of the FIU requires objectivity in decision making, the timely processing of incoming information, and strict protection of confidential data. As the exchange of information between the FIU and law enforcement agencies is based in large part on trust, ensuring the FIU inspires trust from its counterparts (reporting entities), is key to effective co-operation from reporting entities.

To ensure that these requirements are met on an ongoing basis, the FIU needs to be given enough operational autonomy to allow the FIU to carry out their assigned tasks without undue interference.

Financial Action Task Force Recommendation 29 (FATF R29)

FATF R29 confirms the core functions of the FIU are the: receipt, analysis and dissemination of data.

FATF R29 makes no reference to the FIU’s role to include investigations, search or seizure powers.

FIU's role does not including investigation

The AML/CFT Act section 142, does not provide powers to the FIU to make enquiries or investigate. Section 142 explicitly requires matters of investigation to be referred to investigative branches of the NZ Police, or other law enforcement agencies:

- Section 142(e) stipulates the FIU's role is to *analyse* suspicious activity reports and prescribed transaction reports, to assess whether they should be referred to the NZ Police investigative branches, or other law enforcement agencies.

- Section 142(g) reconfirms if a suspicious activity report indicates grounds exist for a criminal investigation, the FIU is required to refer the matter to the NZ Police investigative branches or other law enforcement agency.

The AML/CFT Act intentionally excluded investigation powers from the FIU in order to avoid the FIU from being distracted and committing limited resourcing power to labour intensive functions.

Should the core functions of the FIU become dysfunctional, the entire framework of AML/CFT compliance becomes fractured and ineffective.

Search and Seizure

The sample provided in the consultation question attempts to lessen the significance of this increased power by describing the circumstances as a "request for information". In reality, the Ministry of Justice is seeking to obtain powers of 'search and seizure':

Search – If the FIU is seeking information from a travel agency or airline, this may very well result in the FIU sending written requests to every travel agency and airline. Upon receipt of the request, the travel agency and airline would be obligated to search their data records.

Seizure – Should the travel agency or airline locate the information that the FIU seeks to obtain, the data and record must be provided to the FIU. The FIU is obtaining and therefore seizing this data.

Powers of search and seizure are already provided for in other statues. These strict protocols exist for the purpose of protecting New Zealanders from harsh and authoritarian treatment.

Accountability mechanisms of the FIU need to ensure that the special powers entrusted to the FIU are not compromised. Resourcing of the FIU should be focused intended purposes of receipt, analysis and dissemination of intelligence data.

As the FIU receives information from the private sector without warrant, it would be risky to provide the FIU with additional powers of investigation. Investigation should be left to a law enforcement body such as the criminal investigation branch of the NZ Police. These units are empowered with adequate tools and are governed by laws to ensure any process of obtaining information is fair and proper.

Breach of Bill of Rights

This consultation question needs to consider the rights afforded to New Zealand citizens under section 21 of the Bill of Rights, – *“Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.”*

4.5.2. Providing for ongoing monitoring and transaction of accounts

Consultation Question

- Should the FIU be able to request information from businesses on an ongoing basis? Why or why not?

- If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?

Response

Section 142(e) of the AML/CFT Act explicitly states the FIU's functions are to – _'analyse suspicious activity reports to assess whether any should be referred to investigative branches of the New Zealand Police and to other law enforcement agencies for criminal investigation'.

Investigations are not the role of the FIU.

Further, providing the ability for the FIU to monitor on an ongoing basis, is similar to ongoing surveillance. It is not the role of the FIU to conduct ongoing surveillance. Any power by a law enforcement agency to exercise surveillance would require a warrant. Existing statutory instruments require the grounds for government surveillance to meet the threshold of "reasonable belief" – not suspicion.

The AML/CFT Act is first and foremost a law designed to promote compliance. Attempting to extend the AML/CFT Act to incorporate investigation powers should be strongly opposed. Considerations of oppression and breaches of rights afforded under the Bill of Rights need to be thoroughly considered.

The FIU's role should remain status quo as a data analysis centre – not an investigation arm. Changing its core function has the risk of undermining the effectiveness of the entire AML/CFT framework.

4.5.3. Freezing or stopping transactions to prevent harm

Consultation Question

- Should the Act provide the FIU with a power to freeze, on a time limited basis, funds or transactions in order to prevent harm and victimisation? If so, how could the power work and operate? In what circumstances could the power be used, and how could we ensure it is a proportionate and reasonable power?

- How can we avoid potentially tipping off suspected criminals when the power is used?

Response

Freezing funds or preventing transactions from proceeding, can cause significant financial harm to an individual or third party. This may include financial loss arising from failure to meet deadline dates for settlements relating to investments, or real estate transactions. Any actions that have the potential to penalise an individual or corporate body, must be based on reasonable grounds to believe. The threshold must be higher than ‘suspicion’.

On the basis that the FIU has no power of investigation, the FIU should not be empowered to ‘freeze’ or ‘stop’ transactions.

Any powers to freeze funds should be made by a competent investigation agency, that has formed reasonable grounds to believe that not freezing the funds will result in harm. This protects people from being subject to harsh or oppressive treatment.

Section 21 of the Bill of Rights protects against unreasonable search and seizure – *Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise*.

Section 27 of the Bill of Rights affords the right to natural justice – *Every person has the right to the observance of the principles of natural justice by any tribunal or other public authority which has the power to make a determination in respect of that person’s rights, obligations, or interests protected or recognised by law.*

To ensure protections under the Bill of Rights Act are maintained, any action to freeze funds would first need to establish reasonable grounds to believe that the funds are indeed linked to a predicate crime. This requires investigation. The FIU’s function is not to investigate. Section 142 explicitly requires the FIU to refer matters for investigation to the NZ Police investigation branch or another law enforcement agency.

Excluding the FIU from investigations serves several purposes:

- *Investigations are resource intensive*. The ultimate objective of the AML/CFT Act is for reporting entities to detect and report ML/FT suspicions, that may lead to criminal investigation and prosecution. The framework is therefore highly dependent on the FIU to consistently perform its primary objectives to analyse suspicious activity reports and determine if grounds exist to refer the matter for criminal investigation. As investigations are resource intensive, there is risk the FIU's limited resourcing will impact on its ability to perform its primary function of financial intelligence. By excluding investigations from the FIU's functions, the AML/CFT framework has a greater likelihood of meeting objectives.

- **Reputational damage to the AML/CFT Act**. An investigation branch of a law enforcement agency receives powers from various statutes including the Crimes Act and the Proceeds of Crimes Act. These statues set out criteria that must be met before executing certain powers, such as obtaining a search warrant through written application to a registrar of a court. The grounds must be formed on reasonable belief – not suspicion. These statutes have the purpose of ensuring an investigation is fair and reasonable, not oppressive, malicious or unjust. Freezing funds, even if temporarily, is akin to seizure. By incorporating powers into the AML/CFT Act that are akin to search and seizure, there is the risk that law enforcement agencies will see the AML/CFT Act as an easier, less rigid legal framework, for executing investigation powers. This can easily lead to an abuse of process across law enforcement agencies. Such powers may also result in the AML/CFT Act causing breaches under section 21 and 27 of the Bill of Rights Act.

4.5.4. Supervising implementation of targeted financial sanctions

Consultation Questions

- Should supervision of implementation of TFS fall within the scope of the AML/CFT regime? Why or why not?

- Which agency or agencies should be empowered to supervise, monitor, and enforce compliance with obligations to implement TFS? Why?

Response

AML Supervisors are already obligated to ensure reporting entities are operating with policies, procedures and controls that enable capability for the reporting entity to detect when they may be dealing with, or providing a financial service to, a designated entity in breach of targeted financial sanctions.

This obligation arises from the AML/CFT Act section 39A(b)(iii) which requires a reporting entity to report suspicious activity relevant to the enforcement of the Terrorism Suppression Act (TSA) – *where the reporting entity has reasonable grounds to suspect that the transaction or proposed transaction, the service or proposed service, or the inquiry, as the case may be, is or may be relevant to the enforcement of the Terrorism Suppression Act 2002.*

Sections 9 and 10 of the TSA make it a criminal offence for any person to deal with property that is derived from a terrorist entity or to make property or any financial service available to a terrorist entity.

There is therefore no need to change the AML/CFT Act to empower AML Supervisors to monitor reporting entities for compliance with targeted financial sanctions. This is because the power already exists under Section 39A(b)(iii).

However not all businesses across New Zealand fall under the AML/CFT regime, such as transport and shipping companies, retail outlets etc. There is therefore a significant gap in oversight.

Which government agency should have obligations for educating, supervising, monitoring and enforcing this non AML/CFT sector is for the Ministry of Foreign Affairs and Trade and the Ministry of Justice to determine. This is because both these Ministries have responsibility as Administrators of the TSA.

AML/CFT Supervisors should be prohibited from having any responsibility for business entities that do not meet the definition of financial institution or a designated non-financial business or profession.

4.6. Secondary legislation making powers

Statutory Review Consultation Document

The Act allows for a wide range of secondary legislation to be issued, including regulations (generally issued under section 153 and 154), Ministerial exemptions (section 157), and Codes of Practice (section 64). These powers are intended to allow the regime to be flexible and responsive and allow for changes to be made without amending the Act.

Consultation Questions

- Are the secondary legislation making powers in the Act appropriate, or are there other aspects of the regime that could benefit from further or amended powers?

- How could we better use secondary legislation making powers to ensure the regime is agile and responsive?

Response

Key stakeholders operating under the AML/CFT regime include (a) reporting entities, (b) professional membership groups that represent reporting entities, (c) AML/CFT consultants, and (d) AML/CFT auditors (collectively referred to as *key stakeholders*).

Currently the AML/CFT Act relies on a *Co-ordination Committee* whose role is to ensure the consistent, effective, and efficient operation of the AML/CFT regulatory system (section 151). The Co-ordination Committee (the CC) is represented by government agencies and explicitly excludes any person from the private sector (section 150(2).

Better use of the Co-ordination Committee

It is not possible for the CC to effectively carry out its role of ensuring effective and efficient operation of the AML/CFT regime if it excludes key stakeholders. This is because reporting entities, AML/CFT consultants and auditors are a primary source of information in knowing whether the Supervisory framework is operating ‘consistently, ‘effectively’ or ‘efficiently’.

As most AML/CFT auditors provide services to each sector, they have first hand information and experience for identifying inconsistencies across the three AML Supervisors.

Excluding key stakeholders from representing their concerns or issues to the CC, results in mistrust and gives the perception the regime’s effectiveness is decided on the basis of a bias in favour of government agencies.

Proposed Changes

1. That the CC’s responsibilities include the function of a forum to hear from key stakeholders from the

private sector.

2. That interim determinations from the CC, impacting upon key stakeholders, are published.

3. Key stakeholders (not the public) are invited to respond to the CC's interim determinations.

4. After considering responses from key stakeholders, final determinations of the CC are republished.

5. That determinations from the CC are a source of information to assist the Minister when considering if secondary legislation should be invoked and/or updated.

The above recommendations would:

- assist to improve trust across private sector participants;
- improve the overall integrity of the AML/CFT Act;
- provide the CC with an adequate framework that enables its officials to be informed.

4.6.1. Codes of Practice

Consultation Question

- Are the three Ministers responsible for issuing Codes of Practice the appropriate decision makers, or should it be an operational decision maker such as the chief executives of the AML/CFT supervisors? Why or why not?

- Should the New Zealand Police also be able to issue Codes of Practice for some types of FIU issued guidance? If so, what should the process be?

- Are Codes of Practice a useful tool for businesses? If so, are there any additional topics that Codes of Practice should focus on? What enhancements could be made to Codes of Practice?

- Does the requirement for businesses to demonstrate they are complying through some equally effective means impact the ability for businesses to opt out of a Code of Practice?

- What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool?

Response

Legal Effect of Codes of Practice

Section 67(3)-(5) of the AML/CFT Act requires a court to have regard to a Code before deciding pecuniary penalty. The Code effectively creates ‘law’. Penalties of the Act are severe and include imprisonment and fines of up to $5 million.

Any legal instrument enabling a court to provide a pecuniary penalty, should be established in a manner where there is no risk of impartiality or bias in the making of the instrument.

Though the AML/CFT Act requires public consultation, there is a risk that if the AML Supervisor or their CEO is too close to the development of the Code, the AML Supervisor and/or its CEO may favour prescribed methods that assist them in their role but which cause increased costs or impracticality to reporting entities.

For these reasons, the writing of a Code must ensure impartiality and that there are clear delineations of the ‘legislative’ and ‘judiciary’ bodies. CEOs of Supervisory agencies and the Commissioner of Police, are not sufficiently independent from the administrative and operational arms of the AML/CFT Act.

Should a Code be written in a bias that favours AML Supervisors and is written without proper consideration to the practical application for the business community, the Code effectively creates ‘law’, that is neither fair or just.

Who should be responsible for issuing Codes of Practice

Any responsible parties for issuing Codes need to have sound practical knowledge on the application of the AML/CFT Act so that the proposed Code can be reviewed objectively. This enables those parties to adequately examine, challenge and critique any recommendations to be contained in a Code.

Without requiring responsible individuals to have prerequisite knowledge at the technical and practical level of AML/CFT compliance, there is the risk that the Code cannot meet its objective. This would result in weaknesses to the AML/CFT regime and harm collaboration from the business community.

Other risks from poorly proscribed Codes include reporting entities unnecessarily facing increased and disproportionate compliance costs. Reporting entities would also be left in a vulnerable position of regulatory action, merely as a result of a poorly written Code.

Role of the Co-ordination Committee

Pursuant to section 152(f), a function of the Co-ordination Committee is to – *provide a forum for examining any operational or policy issues that have implications for the effectiveness or efficiency of the AML/CFT regulatory system.*

As the Co-ordination Committee is also represented by each AML Supervisory agency, the Committee is in a better position to understand matters impacting across the AML/CFT compliance industry.

Addressing Conflicts of Interest

CEOs of government departments that operate with an AML Supervisory function will have a close working relationship with the senior management of the AML Supervisory unit. There is the risk that the CEO may be improperly influenced and is therefore not adequately impartial.

Should the Police Commissioner, as responsible person for the FIU, be responsible for issuing Codes of Practice and Guidelines?

The Police force in New Zealand has a recognised reputation that it is under resourced.

As the Police Commissioner has responsibility of oversight of the FIU, there is the risk that the Commissioner may prefer to develop Codes that reduce resourcing commitments and operational costs upon the FIU, by pushing more responsibility to reporting entities.

The Commissioner may have an unrealistic expectation for reporting entities to operate with sophisticated transaction detection systems. This would result in reporting entities incurring increased compliance costs which are disproportionate to the risks they face.

The Commissioner is therefore not adequately separated from the operational aspects of the AML/CFT Act to ensure Codes are impartial and not bias in favour of the FIU.

Recommendations

- As the Ministry of Justice is the Administrator of the AML/CFT Act and Codes are an essential enforcement tool with judicial power of the courts, the authorisation of Codes should remain at Minister level.

- The Co-ordination Committee has existing responsibility for monitoring the efficiency and effectiveness of the AML/CFT regulatory system, including operational and policy issues. The Committee is also represented by each AML Supervisory agency. The Co-ordination Committee should be responsible for identifying the need for Codes, drafting codes and providing recommendations to the Minister of Justice.

- CEOs from AML Supervisory agencies should not have authority to issue codes. This is because their department is too close to the operational aspects of the AML/CFT Act. CEOs are strongly influenced by the managers of their AML Supervisory unit which may result, either intentionally or unintentionally, creating a bias in favour of the CEO's department.

- The Commissioner of Police should not have authority to issue codes. This is because the Commissioner's role is too closely connected to the operational aspects of the FIU. As the FIU has a focus on financial intelligence, the Commissioner's expectation of financial intelligence capability from a reporting entity may be unrealistic and disproportionate to the objectives of the AML/CFT Act.

- The above processes provide a level of trust that systems are in place to protect against bias judgement of AML Supervisors and/or their CEOs and/or the Commissioner.

4.6.2. Forms and Annual Report Making Powers

Consultation Questions

- Should operational decision makers within agencies be responsible for making or amending the format of reports and forms required by the Act? Why or why not?

- If so, which operational decision makers would be appropriate, and what could be the process for making the decision? For example, should the decision maker be required to consult with affected parties, and could the formats be modified for specific sectoral needs?

Response

The effective application of the AML/CFT regime relies on the free flow of data between reporting entities to AML Supervisors and the FIU. As the financial services industry is evolving rapidly, there has to be flexibility to adapt to changes in data requirements. The results will be a better outcome of the AML/CFT framework, enabling intelligence-led decision making from the government agencies.

The greatest impediment to the effective operation of the AML/CFT Act is the overprescribed detail required from reporting entities. It is therefore important for any prescribed data requirements to be readily available from reporting entities.

Determining Data Quality

Getting the balance right between too much and not enough data will be crucial for the objectives of the AML/CFT Act to be achieved.

The responsible government agencies will need to determine data that is considered necessary in order for them to conduct their role, against data that is ‘nice to have but not necessary’.

Any request for mandatory data will first require government agencies to undertake a cost effective analysis to determine to what extent will reporting entities need to adapt or modify their existing systems in order to obtain the necessary data. This may require thematic reviews or research surveys in order to understand what is the proportion of businesses that already have the existing data, against those businesses that don’t.

Availability of Data

Data is either available or is not available. Therefore reporting entities already have the data, or the request is unable to be complied with because the data does not exist. For reporting entities that do not have the available data, there may be significant costs and resourcing commitment in order to obtain the data. This would be the case for data linked to customers. Ordinarily required data is obtained at time of customer onboarding. If data impacts on existing customers, there were be significant problems for businesses to try

and obtain data retrospectively.

Recommendations

For the purpose of effective data analysis, government agencies will need to:

- inform their data requirements through intelligence-led decision making
- identify what data is necessary, against what data is preferred but not compulsory;
- determine the proportion of businesses operating without the required data;
- determine a realistic timeframe for business to obtain the missing and necessary data;
- conduct a cost benefit analysis of making data mandatory;
- ensure any data requests are not overly prescriptive and unreasonable under the risk based AML/CFT framework.

4.6.3. AML/CFT Rules

Consultation Questions

- Would AML/CFT Rules (or similar) that prescribed how businesses should comply with obligations be a useful tool for business? Why or why not?

- If we allowed for AML/CFT Rules to be issued, what would they be used for, and who should be responsible for issuing them?

Response

Codes have a better application in a risk-based environment in comparison to Rules. This is because Codes enable businesses to achieve the objective of the Code, but in a different approach.

In the application of AML/CFT laws, it is important to ensure businesses retain the flexibility in achieving regulatory outcomes, without following a tick-based approach. Flexibility promotes innovation and enables small businesses to compete on an even playing field.

Because Codes focus on an outcome, under risk-based legislation, Codes should always be preferred over Rules that are designed to be prescriptive.

Rules have the risk that the letter of the law will be followed, but not the spirit of the law. This defeats the risk based approach and may result in businesses following a tick box exercise and fail to evaluate the objectives of why the Rule exists.

The prescriptive approach to compliance laws is becoming less common.

Prescriptive rules in AML/CFT laws primarily serve to provide certainty to businesses so that they have knowledge of regulatory expectation. In particular, small businesses who lack internal expertise find comfort in having a clear line drawn on what they are expected to do. However in the context of New Zealand’s environment, guidelines serve this purpose.

Recommendation

- NZ already operates with a system by application of Codes that serve as similar purpose to Rules.

- Codes are more applicable to the risk based management system, which focuses on outcomes and provides flexibility to achieve the outcome in a manner that is less cost. This is highly relevant to small businesses.

- Rules will disadvantage innovative businesses and discourage the ‘Think smarter’ aspect of conducting business.

- Rules are more likely to result in the letter of the law being met but not the spirit of the law. Therefore the principles based application of AML/CFT laws will be undermined.

- Rules based legislation is more likely to advantage large businesses who have greater resourcing to invest in requirements that are mandatory by law but disadvantage small businesses who have less resourcing. This discourages innovation. The risk based approach is about promoting innovation and avoiding a ‘tick box exercise’.

4.7. Information Sharing

Statutory Review Consultation Document

The FIU maintains a wealth of information that may be relevant to other agencies, including the AML/CFT supervisors. However, the FIU is currently only able to share information with other government agencies on a case-by-case basis. This is administratively burdensome for the FIU, and means that, as a regime, we are unable to realise the full value of the information that FIU holds to support better regulation, supervision, and law enforcement outcomes.

Section 139A of the Act allows for regulations to be issued that enable information sharing, which could include enabling direct data access arrangements. A direct data access arrangement would enhance the overall effectiveness of the regime and how the FIU operates. However, we are also conscious that such an arrangement would have significant privacy implications, as it would allow more government agencies to directly access information that FIU holds (such as SARs and prescribed transaction reports).

New Zealand’s Mutual Evaluation Report (page 44)
The FIU is encouraged to establish ways for government agencies to directly access financial intelligence information from its databases. This would allow the FIU to reallocate resources away from responding to queries, and towards developing more detailed value-added intelligence products.

4.7.1. Direct data access to FIU information for other agencies

Consultation Questions

- Would you support regulations being issued for a tightly constrained direct data access arrangement which enables specific government agencies to query intelligence the FIU holds? Why or why not?
- Are there any other privacy concerns that you think should be mitigated?
- What, if any, potential impacts do you identify for businesses if information they share is then shared with other agencies? Could there be potential negative repercussions notwithstanding the protections within section 44?

Response

Principles of AML/CFT Laws

AML/CFT laws are designed to promote collaboration between the private sector and government. The purpose is for the detection and prevention of money laundering and/or terrorism financing. The laws are designed to get the balance right between protecting national security, whilst having regard to the fundamental principles of privacy laws.

Diminishing the controls around privacy principles within New Zealand's AML/CFT Act will result in a backlash from the public, and reporting entities, who are strong in enforcing privacy principles. The public represent the customers and reporting entities represent the businesses where the customers trade. If fundamental rights to privacy and protection of personal data are compromised, the end results will see government struggle to promote collaboration within the private sector, reducing the overall effectiveness of the AML/CFT Act. By weakening collaboration with the private sector, this will in turn remove one of the most powerful tools that government have for detecting ML/FT. Protecting fundamental rights of privacy must therefore continue to be a cornerstone in the legislation.

Principles of Privacy Laws

Privacy is protected as a human right at the highest international level.

Privacy laws are an essential means to protect individuals against arbitrary and unjustified use of power.

The right to privacy is articulated in all of the major international human rights instruments, including:

- United Nations Declaration of Human Rights (UDHR) 1948, Article 12: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Principles of Privacy Laws in context of AML/CFT laws

As AML/CFT laws operate under a veil of secrecy, the laws are purposely designed to provide robust controls around the protection of privacy principles. These robust controls recognise that should an individual's privacy be materially compromised, the individual will be completely oblivious of the breach existing. This is due to AML/CFT laws requiring strict confidentiality around the submission of suspicious activity reports sent from businesses to FIUs.

Whereas ordinarily a principle of privacy laws allows individuals the right to seek information held about them and correct the inaccurate information, this is not possible under AML/CFT laws. Under AML/CFT laws an individual does not have the right to seek information that the FIU holds about them. Therefore there is the real risk that inaccurate information may result in an unjustified monitoring against the individual, and the individual has no capability or opportunity to question these activities. The inaccurate information may have been unintended, or it may have been intended with a malicious or corruptible purpose.

New Zealand's Context

New Zealand is a jurisdiction that recognises the need and fundamental rights to promote and protect an individual's right to privacy of personal information. These laws are contained in the Privacy Act 2020 and the Bill of Rights Act 1990. Both laws are designed to prevent violations of human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

Additional to the Privacy Act 2020 and the Bill of Rights Act, New Zealand has obligations to international treaties that develop minimum standards and have the purpose of protecting human rights. This includes the Convention on the Organisation for Economic Co-operation and Development (OECD) and the International Covenant on Civil and Political Rights.

Explicit Protection of Personal Information

The AML/CFT Act is explicit that it seeks to protect the sharing and disclosure of personal information:

New Zealand's AML/CFT Act recognises these fundaments rights of privacy. If the RBNZ, the DIA and the FMA obtain privacy information whilst performing their role as an AML Supervisor, they are prohibited from using the personal information for any other role they are responsible for (section 137).

The Police Commissioner, the NZ Customs Service and AML Supervises are authorised to disclose information to a government agency or law enforcement agency, but prohibits disclosure of privacy information (section 139).

When can personal information be disclosed?

The AML/CFT Act allows disclosure of personal information only when the definition of 'Law Enforcement Purposes', as contained in Section 5, is present. The definition of *'Law Enforcement Purpose'* means:

(a) the prevention, disruption, detection, investigation, and prosecution of—

(i) any offence under this Act; or
(ii) a money laundering offence; or
(iii) any offence within the meaning of that term in section 243(1) of the Crimes Act 1961; or
(iv) an offence under the Terrorism Suppression Act 2002:

(b) the enforcement and administration of—
(i) this Act:
(ii) the Criminal Proceeds (Recovery) Act 2009:
(iii) the Misuse of Drugs Act 1975:
(iv) the Terrorism Suppression Act 2002:
(v) the Mutual Assistance in Criminal Matters Act 1992:
(vi) the Customs and Excise Act 1996:

(c) the performance by the New Zealand Security Intelligence Service or the Government Communications Security Bureau of its functions under the Intelligence and Security Act 2017:

(d) the detection and prevention of the harms specified in section 58(2) of the Intelligence and Security Act 2017:

(e) any purpose or action referred to in paragraphs (a) to (d) relating to, or taken in respect of, legislation of an overseas jurisdiction that is broadly equivalent to the enactments referred to in those paragraphs.

The above definition of *'law enforcement purposes'*, confirms the primary objective of the AML/CFT Act is to detect serious crimes that have the potential to impact upon New Zealand's national security.

Further, Section 3 clarifies the purpose of the AML/CFT:

Purpose
(1) The purposes of this Act are—
(a) to detect and deter money laundering and the financing of terrorism; and
(b) to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and
(c) to contribute to public confidence in the financial system.

(2) Accordingly, this Act facilitates co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies.

The definition of law enforcement purposes confirms disclosure of privacy information must be for offences liked to money laundering and/or terrorist financing. Obviously this is why it is named the *Anti-Money Laundering and Countering Financing of Terrorism Act*.

Privacy Act 2020 versus the AML/CFT Act

Whereas Principle 11 of the Privacy Act allows the disclosure of personal information for *'avoiding prejudice to the maintenance of the law'* and for *'law enforcement purposes'*, the AML/CFT Act overrides Principle 11

by defining the meaning of ‘law enforcement purposes’. The definition is contained in Section 5.

Defining *law enforcement purposes* was an intended statutory override of Principle 11. The statutory override ensures any disclosure of personal information is in context of preventing money laundering and/or terrorist financing.

The definition of *law enforcement purposes* in Section 5 recognises that the AML/CFT Act empowers businesses to collect extensive and intrusive personal information pertaining to their customers. There is no limitation to the amount of personal and private information that a business may seek from its customer. The business has discretion on the amount of detail required under obligations of *customer due diligence* and *ongoing customer due diligence* (sections 9-31). Information to be disclosed may include passports, driver licenses, bank statements, detail of family trusts (objectives, assets and beneficiaries), net worth of individuals, sources of wealth and sources of funds.

Prior to the implementation of the AML/CFT Act, there was no other existing law in New Zealand that enforced the private sector to be so intrusive into the personal aspects of their customers. The intrusive nature of the AML/CFT Act, was the reason why the AML/CFT Act was required to have transparent and rigid controls around sharing and disclosure of personal information. The AML/CFT Act achieved this by defining the meaning of *‘law enforcement purposes’*.

The context of the AML/CFT Act being an override of Principle 11 is clear and non-debatable. It does not take a legal scholar to make this finding.

Context of *Law Enforcement Purposes*

When the AML/CFT Act’s definition of *‘law enforcement purposes’* is present, it provides government agencies with extreme powers that authorise:

- The NZ Police, the New Zealand Securities and Intelligence Service, or the Government Communications and Services Bureau, to establish an account with a reporting entity using a false customer name and operate with customer anonymity (Section 38(2)(b));
- A police employee to disclose information within a suspicious activity report (section 46(3));
- An AML Supervisor may disclosure a suspicious activity report to the NZ Police (section 46(4));
- Any person may disclose a suspicious activity report to the NZ Police (section 46(8));
- AML Supervisors may disclose personal information concerning employees or senior managers to the NZ Police (section 48(a));
- Reporting entities may share information with regulators and law enforcement agencies in accordance with regulations made under section 139A; (NB: presently, no regulations have been made);
- Enable the Police FIU to receive information from international authorities (section 142(ka)).

All the above circumstances first require the definition of ‘law enforcement purposes’ to be present. Should any circumstance exist that does not meet ‘law enforcement purposes’, the AML/CFT Act explicitly prohibits the disclosure of personal information.

Power to Disclose

Section 139 of the AML/CFT Act provides provisions of ‘Power to Disclose’ and contains three sub-sections.

Section 139(1) – allows the Commissioner of Police and the NZ Customs Service or an AML/CFT Supervisor to disclose any information (**that is not personal information**) to any government agency, or any regulator, for **law enforcement purposes**. The emphasis are mine and confirm that:

- AML/CFT agencies are preventing from disclosing privacy/personal information.
- Information that is not personal information may be disclosed only for ‘law enforcement purposes’ as defined in the AML/CFT Act.

Section 139(2) requires regulations to be made before reporting entities are authorised to disclose any information to a government agency or regulator. Any information so disclosed is required to meet definition of ‘law enforcement purposes’.

Section 139(3) states – *Nothing in this section limits the Privacy Act 2020 (which permits certain disclosures in addition to those authorised under this section).*

Section 139(3) is unclear of its intended meaning, however, it appears to be confirming any such disclosures under section 139 must still consider requirements of the Privacy Act The same string of words can also be found in other statues including (but not limited to) the – (a) Fuel Industry Bill, section 28(5), (b) the Takeovers Act 1993, 15A(4), © the Fair Trading Act 1986, section 48A(4), (d) the Companies Act 1993, section 371A(4), (e) Health and Safety at Work Act 2015 197(4).

It would be absurd to interpret that section 139(3) authorises Principle 11 of the Privacy Act to override the AML/CFT Act. Such an interpretation would result in the AML/CFT Act having a primary purpose of detecting and preventing every conceivable crime that exists in NZ laws. It would also mean every law enforcement and regulatory agency in New Zealand has powers to obtain personal information when the Commissioner of Police is prohibited from doing so (section 139(1).

Finally, if it was intended for every law enforcement or regulatory agency to have access to personal information collected under the AML/CFT Act, there would be no need for section 139(2). Section 139(2) requires the Governor General to authorise regulations for the sharing of information from and between reporting entities and law enforcement agencies.

Summary – restrictions for sharing personal information

The submissions above provide clear references, contained in the AML/CFT Act, that:

- Prohibits law enforcement agencies, or regulators, from seeking or obtaining, personal information

from reporting entities, when the personal information was obtained under powers of the AML/CFT Act.

- Any information disclosed or shared with law enforcement agencies, must first meet the definition of ‘law enforcement purposes’, as defined in Section 5 of the AML/CFT Act.

- Unless authorised by regulations, reporting entities are prohibited from disclosing personal information or any information, to law enforcement agencies or regulators (s.139(3)).

Ongoing Breaches of the AML/CFT Act by law enforcement agencies

In Q2 of 2021, I became aware of breaches of the AML/CFT Act involving government agencies, including the Serious Fraud Office and the Overseas Investment Office. These government agencies provided written requests for disclosure, seeking information and personal information from reporting entities. Their requests did not meet the definition of ‘law enforcement purposes’, as contained in Section 5 of the AML/CFT Act.

I reported my concerns to the Department of Internal Affairs (as the relevant AML Supervisor), seeking clarification of the situation. I set out my concerns in writing via email and advised that as the matter did not include ‘law enforcement purposes’, the reporting entity, pursuant to section 139(2), was not authorised to release the information. I advised in the email that loose controls around disclosure could result in acts of corruption.

Though I provided my concerns in writing and had expected a reply in writing, Instead the DIA phoned me. During our discussions they acknowledged that the matter was unclear. I asked if they could provide a reponse in writing so that I could provide certainty to my client.

The written response that I received from the DIA did not address the issue. The response was ambiguous and did not provide clarity. The response said any disclosure “… must be made in conjunction with a lawful request.” There was no mention of the relevancy of ‘law enforcement purposes’. The response was unhelpful and did not assist the reporting entity to understand their compliance obligation.

I then sent a further written reply to the DIA, highlighting that as an AML Supervisor they had an obligation to – *provide guidance to the reporting entities it supervises in order to assist those entities to comply with this Act and regulations* (section 131 (c).

I also turned to the Ministry of Justice (as Administrator of the AML/CFT Act), seeking clarification on the issues. I highlighted that my request was urgent as the reporting entity had been given a timeline by the law enforcement agency to reply. Seven weeks after sending that request, I received a detailed response from the Policy Manager of Criminal Justice (PMCJ) from the Ministry of Justice.

The email from the PMCJ, is in my view, an example of how government departments, including the Ministry of Justice as Administrator of the Act, will collaborate for the purpose of enabling law enforcement agencies to exploit the AML/CFT. They will go to any extent, including providing false information and intimidate industry stakeholders and reporting entities with threats of legal action if they do not comply, when in fact compliance would cause a breach of the AML/CFT Act.

As a former regulator and investigator with familiarity of powers to make written requests for disclosure, I am aware of the extreme advantages that the AML/CFT Act provides to law enforcement agencies. Before the implementation of the AML/CFT Act, which occurred on 1 July 2013, the private sector had no mandatory legal obligation to inquire intrusively into the personal lives of their customers. The AML/CFT Act changed that – considerably. Under the AML/CFT Act, there is no limitation on the extent of personal information that a business can now obtain from their customers. Decision making is meant to be based on risk. The greater the risk that the customer presents to potential threats of facilitating ML/FT, the greater the level of customer due diligence that the business conducts.

Guidelines from AML Supervisors are that if a customer does not wish to comply with requests, consideration of submitting a suspicious activity report should be considered. In these circumstances, the customer may choose not to comply with the requests for personal information, simply by being insulted by the intrusive nature of requests. The customer instead may choose to take their business elsewhere. However, their refusal to provide personal information could be considered suspicious, resulting in monitoring and surveillance by law enforcement over that person's financial activity.

This was the reason why the AML/CFT restricted the powers for government agencies to share and disclose personal information. The AML/CFT Act achieves this by ensuring that any disclosure or sharing of information is for the purpose of detecting offences of money laundering and terrorism financing. This was the reason for providing a definition of 'law enforcement purposes' (s.5 of the AML/CFT Act).

Seven weeks after I made an urgent request to the MoJ, its PMCJ replied in writing, within one business day after I had received threats from the government's legal representative, threatening legal action if the reporting entity did not comply. The PMCJ's email made a number of erroneous statements, which are clearly contrary to the AML/CFT Act:

- The effect is that AML/CFT Act does not anticipate that AML/CFT information, with the exception of information relating to SARs/PTRs, will be more protected than any other private information.
- The intention was not to restrict information sharing by section 139(2) provision; nor was it intended to affect the scope of information sharing in the absence of regulations made under section 139A.
- Even in the absence of the background to the policy intention, a plain reading of section 139(2) does not, in our view, support your reading that the Governor General must authorise information by Order in Council before a reporting entity or government agency can share information (if not explicitly provided for by the Act).
- The definition of law enforcement is not likely to have much bearing on your client's obligations.
- The clear policy intent is to link the meaning of law enforcement to detection etc of all predicate offences (ie, any offence).
- The AML/CFT Act does not have a framework of authorising access. Authorisation to access comes from the Privacy Act and/or the Search and Surveillance Act and/or the agencies' specific legislation.
- However, if section 139(2) were brought into effect by regulations, it is our view that the limitation to law enforcement purposes would therefore include prevention, disruption, detection, investigation, and prosecution of any predicate offence.
- The definition of law enforcement in the AML/CFT does not have a bearing on other Acts; such as the scope of the SFO powers in the SFO Act.
- None of the sections of the AML/CFT Act have any bearing on restricting disclosure of personal

information (other than suspicious activity report and prescribed transaction reports).
- There are no provisions that provide additional protections to information collected for CDD beyond the Privacy Act.
- You might be interested to know, if you don't already, that MOJ is required to conduct a statutory review of the act during 2021-22 (section 156A refers). The arrangements for consultation have yet to be agreed by the Government, but this will certainly involve public consultation. If you think that the provisions are not functioning properly, this consultation would be a good opportunity for you to provide feedback.
- I appreciate your feedback; however, having reviewed your messages and letter, I am confident that this view is based on misunderstandings of statutory roles, the function of the Act and the machinery of government generally.
- In any case, submission on the statutory review would provide a better mechanism for you to voice your opinion.

It is clear the advice from the MoJ was erroneous and I believe is an example of an abuse of power. It is also clear to see that the government agencies are desiring to change the AML/CFT Act to move away from the detection, prevention and investigation of money laundering and terrorism financing and enable the AML/CFT Act to be used to detect, prevent and investigate any crime. This is absurd and I ask the Parliamentary Steering Committee to note that this should strongly be opposed.

To support my views that the advice from the MoJ was wrong, I refer to the 2017 regulatory impact statements and also the submission from the Privacy Commissioner. The 2017 amendment of the AML/CFT Act, was in preparation for the introduction of lawyers, accountants and real estate agents. At this time the MoJ had intended to change the meaning of *law enforcement purposes* to have a far wider reach. The MoJ's intention was to enable regulators and law enforcement agencies the capability of obtaining and sharing information from AML Supervisors, the FIU and reporting entities.

After reviewing various documents that were created at the time of the 2017 amendment of the AML/CFT Act, I have become aware that the MoJ is not impartial in its legislative recommendations in that it does not properly consider and report on the impact and changes of fundamental human rights. The MoJ attempts to mislead Select Committees by not properly informing Parliament Select Committees of the fundamental changes that their proposals make. It is clear, in my opinion, the MoJ is improperly influenced by government agencies, at the expense of democracy.

Thank goodness there is the requirement before legislation is passed for Cabinet to receive input from the Privacy Commissioner. If it was not for the Privacy Commissioner's input, the 2017 Parliamentary Select Committee would have progressed to change NZ's AML/CFT Act into an instrument that enabled government agencies to have repressive control over the information that the private sector now hold.

Privacy Commissioner's submissions to the Law and Order Committee

During the 2017 review of the AML/CFT Act, the Privacy Commissioner provided submissions which strongly opposed the widening of sharing information between government agencies. The Privacy Commissioner noted there were not proper safeguards in place to extend the powers of the AML/CFT Act.

Though the MoJ had sought to extensively widen information sharing and amend the definition of 'law enforcement purposes', the Privacy Commissioner's recommendations prevented that from happening. The result was the definition of 'law enforcement purposes' was not changed and sharing of information between reporting entities and law enforcement agencies required an Order in Council from the Governor General (s.139(2)).

The below statements have been copied from the Privacy Commissioner's submissions. The Privacy Commissioner's statements confirm that the communication to me from the MoJ's Policy Manager of Criminal Justice were wrong and misleading.

Summary of Privacy Commissioner's Submission

- This submission focusses on the provision in the Bill that give new and expanded powers for agencies to share information, including personal information. These provide for the collection and disclosure of the personal information of a significant number of individuals and will therefore have significant implications for personal privacy.
- My view is that the framework for information sharing provided under clauses 38, 40 and 48 is confusing, contains unnecessary duplication, and gives disproportionate powers to agencies to share information in a way that goes beyond the objectives of the Bill and risks undermining privacy protections in other statutes.
- Amend the definition of "law enforcement purposes" in clause 5 to ensure that it cannot be read broadly to include functions outside the purposes of the AML/CFT regime and to ensure that information sharing authorised by officials is appropriately constrained;
- Amend the Bill to create a single regulation making power, with appropriate safeguards, related to information sharing;
- Remove section 140A from the Bill and instead require agencies to seek approval for direct access arrangements through Order in Council, either under a regulation making power referred to above or through the approved information sharing agreement mechanism contained in Part 9A of the Privacy Act 1993;
  • Ensure concerns identified in the Privacy Impact Assessment conducted for this Bill are addressed before the Bill progresses.
- I was pleased to have the opportunity to comment on an Exposure Draft of the Bill, and note that the Bill includes some changes that reflect the comments I made during that consultation. However, substantive changes have been made to the information sharing provisions which means that, compared to the Exposure Draft, I no longer view them as proportionate nor the safeguards as adequate.
- I consider the information sharing regime provided for under the Bill as currently drafted is ill-defined, overly broad and goes well beyond what is necessary to give effect to the Shewan Report's recommendations or to provide for an effective and efficient AML/CFT regime.
- The information sharing provisions in clauses 38, 40 and 48 go beyond what is necessary to give effect to the recommendations of the Shewan Report, and would give disproportionate powers to officials to share personal information. They are also confusing, giving multiple mechanisms under which information sharing can occur, with some mechanisms containing considerably fewer safeguards than others, without apparent justification.
- The definition of "law enforcement purposes" in the Bill is very broad. It expands the current definition,

meaning the new sections 139(1) and (2) give officials a disproportionate power to share personal information with a very wide range of agencies.
- The expanded definition is problematic. The lack of specificity …. create the risk of inappropriate information disclosure outside of the purposes of the AML/CFT regime.
- Legislative authority for officials to share personal information, without oversight by Ministers or Parliament, is only appropriate where the purposes for disclosure are clearly defined and limited. I therefore recommend that the definition of "law enforcement purposes" in the Bill be refined to ensure that it is clearly restricted to activities related to the AML/CFT regime, and cannot be read inappropriately broadly.
- If the intention is to allow officials to share information for broad purposes, then I recommend that additional safeguards included, such as that information sharing arrangements can only be approved by Order in Council following consultation with the Privacy Commissioner.
- New section 139(3)(b), states that in the absence of regulations, information sharing can be authorised by a written agreement between agencies.' Why section 139(3)(b) is required is not clear, given the ability to share information under sections 139(1) and (2). This (new) section would appear to create an avenue for officials to avoid the requirement to seek regulations under sections 139A or 153, thus bypassing any Ministerial or Parliamentary oversight. I therefore recommend that new section 139(3)(b) be removed from the Bill.
- It is not clear why such a broad power to allow direct access is required for the purposes of the AML/CFT regime, nor why the power to enter into written agreements should be delegated to officials rather than being approved by Order in Council. No other public sector chief executives have the authority to enter into agreements that override people's privacy rights in this way. I note that all government agencies have access to the approved information sharing agreement mechanism contained in Part 9A of the Privacy Act 1993. This mechanism can be used to authorise direct access arrangements and includes appropriate safeguards.

Following the Privacy Commissioner's submissions, all recommendations were accepted which resulted in a significant change to the draft Bill. Though the draft Bill sought changes to the definition of 'law enforcement purposes', the Privacy Commissioner's recommendations prevented that from happening.

The Regulatory Impact Statement on the 2017 review

The Regulatory Impact Statement 2017 (RIS 2017) also confirms that the communications to me from the MoJ's Policy Manager for Criminal Justice was wrong and misleading. Highlights of the RIS 2017 support my view as provided below:

Paragraph 168
The AML/CFT Act provides a prescriptive regime for sharing information. In general, Police and the FIU, Customs and the AML/CFT supervisors (the AML/CFT agencies) are able to share information, but the process for sharing is highly prescribed. The AML/CFT agencies can share information with other agencies only in limited circumstances:

- where the information shared is not personal information; and
- where the information is shared for law enforcement purposes.

Paragraph 169

- The restriction to non-personal information for agencies other than AML agencies greatly restricts the information that can be shared and therefore the value of the sharing; agencies with a clear interest in AML (e.g. Inland Revenue) are excluded.

- Limiting the purpose to law enforcement purposes has constrained the flow of information and excludes, for instance, information that is relevant to supervision or other regulatory management, but not a crime;

Current and Ongoing Systemic Breaches by Government Agencies

Law enforcement agencies and regulators have recognised the extraordinary powers under the AML/CFT that require the private sector to collect and store extensive personal information from their customers. They are using their internal regulatory powers that are outside the real for detection of ML/FT and using the AML/CFT Act as a back door to support their investigation units. This back door approach in my view is unlawful.

As my client was threatened with legal action, increased compliance costs and the likelihood of harm to reputation for refusing the request, my client was put in a position of providing the information sought, with knowledge that such authorisation was not lawful under the AML/CFT Act.

These circumstances highlight that the DIA and the MoJ are not fulfilling obligations to ensure the industry have sufficient information to understand their regulatory obligations. Under section 131 (c), AML Supervisors are compelled to provide guidance to the reporting entities it supervises in order to assist those entities to comply with the Act and regulations.

As the controls around information sharing are a key aspect for the proper administration of the AML/CFT Act, guidance from AML Supervisors should have already been provided on this matter. Omitting to provide guidance to the industry is exposing reporting entities to knowingly or unknowingly committing breaches of the AML/CFT Act under provisions of sharing and disclosing information to law enforcement or regulatory agencies.

When I first sought confirmation from the DIA to clarify the context of the meaning of ‘law enforcement purposes’ to the disclosure request, the DIA’s initial response by phone was that it was not clear. A further written response failed to clarify the issue and advised the reporting entity should seek legal advice. Seeking legal advice would have significantly increased compliance costs for the small sized business. Not only would legal advice significantly increase costs, it would not have been provided in the timeframe allocated that the request for disclosure provided.

The DIA’s sector represents 60% of reporting entities falling into the category of ‘small’. A key aspect of AML/CFT compliance is that compliance costs must be proportionate to the size of the business. Where a large institution may have a team of legal advisers at their disposal, a small size business does not. It is for these reasons that the AML/CFT Act obligates AML Supervisors to assist entities to understand their compliance obligations. This is only one example in which I assert the DIA is failing its role as an AML

Supervisor and the MoJ is failing in its role to Administer the AML/CFT Act without a bias.

Direct Access from Law Enforcement Agencies to FIU Database

This public consultation is seeking to allow direct data access to FIU information from law enforcement agencies.

The recent country inspection of NZ's systems, conducted by the international watchdog, the Financial Action Task Force, seems to indicate this practice is already occurring. The FATF's mutual evaluation report advises -

- Law enforcement agencies obtain financial information from the FIU, via direct access to the goAML database and through requests to financial institutions and designated non-financial business professionals (page 43 of FATF report).

- The FIU should incorporate a tracking/feedback mechanism into its case management which tracks the use of FIU products and financial intelligence directly accessed by law enforcement agencies (Page 46 of FATF report).

- The remaining 80% of reports are not individually reviewed, though they do form part of the FIU database, and therefore are available to be analysed and disseminated in response to law enforcement agencies' request for SAR information (paragraph 159).

Finally on this point, I note that the Policy Manager for Criminal Justice was previously the Head of the NZ Police FIU. It concerns me that there might be improper influence from within the MoJ to extend the powers of the AML/CFT, in favour of law enforcement agencies. Such extension of powers would be at the expense of breaching fundamental human rights and eroding New Zealand's democratic values. It also creates real risk that the reputation of NZ's AML/CFT laws will be permanently harmed.

4.7.2. Data matching to combat other offending

Consultation Document

Information that is held by the FIU could also be used to combat other offending more effectively if it is matched with data that other government agencies hold. For example, prescribed transaction reports could be matched with trade data held by Customs to identify suspicious cross-border trade transactions that may indicate trade-based money laundering.

However, data matching has significant privacy implications as it uses personal information for purposes other than what it was collected for. If we develop data-matching arrangements, we will need to carefully navigate these privacy considerations and ensure that relevant FIU data is matched in specific and limited circumstances.

Consultation Questions

- Would you support the development of data-matching arrangements with FIU and other agencies to combat other financial offending, including trade-based money laundering and illicit trade? Why or why not?

- What concerns, privacy or otherwise, would we need to navigate and mitigate if we developed data-matching arrangements? For example, would allowing data-matching impact the likelihood of businesses being willing to file SARs?

Response

The FIU’s role is to receive, analyse and disseminate financial intelligence. The FIU under its current powers and systems already has capability to provide data-matching and improve intelligence for government agencies who have a role to prevent money laundering and financing of terrorism. The FIU is able to improve financial intelligence for those government agencies, without needing to share personal information.

The concerns are that before the FIU is provided greater power, the Commissioner of Police must first provide an AML/CFT infrastructure that instills trust to the private sector or stakeholders, and meets the objectives of the AML/CFT Act.

Antiquated Systems

When a reporting entity or DNFBP is obligated to send a suspicious activity report, the goAML system provided by the FIU requires the business to commit extensive resourcing and it can take up to half a day (4 hours) or more to submit one report. Most often the report is ‘rejected’ and automatically sent back to the business. The reason for the rejection is never clear and requires the business to commit even further resourcing.

In order to promote proactive reporting, businesses must have a system that is user friendly and enables a suspicious report to be submitted within 30 minutes, and no more than an hour. Any time commitment greater than that will cause reporting entities and DNFBPs to avoid reporting – thereby defeating the primary objective of the AML/CFT Act.

goAML not fit for purpose

The AML/CFT Act requires suspicious activity reporting of customers, as well as **proposed** customers (section 39A(a)(ii) and 39A(b). Capturing a *proposed* customer means that should a potential customer take steps and make an inquiry to establish a business relationship but during the onboarding process decide they no longer want to proceed, this may prompt a business to have a 'suspicion' and desire to submit a suspicious activity report.

Unless the business has in their possession specific customer data, the goAML system will prevent the business from providing a suspicious report. An example not having the customer's date of birth available. If a date of birth is not available, the goAML system denies the submission.

As the AML/CFT Act requires detection of suspicions from 'proposed customers', the systems needs to be more flexible and recognise that certain data of 'proposed' customers may not be available.

I am aware this issue has resulted in the goAML system preventing reporting entities from submitting suspicious activity reports.

goAML system breaching AML/CFT Act

I provide another example to highlight the goAML system is not fit for its proper purpose.

As a previous user of the goAML system I received into my goAML account a number of SARs and PTRs from another reporting entity. I immediately reported it to the FIU who confirmed it was a glitch and apologised. However, the FIU through failure of the goAML system, had inadvertently breached the AML/CFT Act by disclosing a suspicious activity report to a person that was not authorised.

Was this the first and only time this breach had occurred or has it happened before? Is the risk still there for the some issues to re-occur?

Governments not committing investment to infrastructure

There are increasing requests for reporting entities to operate with sophisticated systems of transaction monitoring, yet the FIU is using basic analysis tools, such as keyword searches and only analysing 20% of suspicious reports received. 80% of reports are not individually reviewed (FATF MER paragraph 159).

Whereas businesses have incurred significant expense to play their part in making New Zealand a safer country to conduct business, the same cannot be said for the FIU agency.

The business community need to be encouraged to be proactive in making suspicious reports. If the results are they have to use a system that can take up to half a day or more for one report, then the AML/CFT Act

has failed. A government owned system that fails the private sector cannot promote harmony and co-operation between the private and public sectors.

If the business community are being encouraged to report but the FIU are not analysing 80% of reports received, then again – the AML/CFT Act has failed and it is likely suspicious reports qualifying for grounds to investigate ML/FT, have not been identified.

Ongoing breaches of sharing information

The AML/CFT is explicit that privacy information cannot be shared with law enforcement agencies (LEAs) and neither can suspicious activity reports (SARs), yet the FATF mutual evaluation report confirms that LEAs are accessing the goAML FIU database directly:

- Law enforcement agencies obtain financial information from the FIU, via direct access to the goAML database and through requests to financial institutions and designated non-financial business professionals (page 43 of FATF report).

- The remaining 80% of reports are not individually reviewed, though they do form part of the FIU database, and therefore are available to be analysed and disseminated in response to law enforcement agencies' request for SAR information (paragraph 159).

To aggravate the situation, the FIU are unable to track and audit who is accessing the SAR database:

- The FIU should incorporate a tracking/feedback mechanism into its case management which tracks the use of FIU products and financial intelligence directly accessed by law enforcement agencies (Page 46 of FATF report).

Risk of Corruption

The AML/CFT Act is a powerful piece of legislation and I would suggest, one of the greatest tools available for attempting to combat money laundering and terrorism financing – crimes that effect all New Zealanders.

My experience is that government agencies are not committing adequate resourcing to their roles, and are using improper and at times, unlawful practices that breach the AML/CFT Act.

Corruption, bribery and money laundering are in parallel. Corruption and bribery can assist launderers evade detection. New Zealand is highly exposed to the threat of corruption and bribery. We are a country without a dedicated anti-corruption agency.

In the context of the AML/CFT Act enabling the private sector to collect intrusive personal information from its customers, until the FIU is independently reviewed to confirm the status of basic expectations are met, no additional powers should be provided. These controls protect New Zealanders from regressive government actions that threaten improper and/or unlawful breaches upon their basic human rights.

5. Supervision, regulation, and enforcement

Consultation Document

A core component of the AML/CFT regime is that it needs to enable effective supervision and regulation of businesses. The supervision and monitoring of businesses should address and mitigate money laundering and terrorism financing risks in the economy, in part by promptly identifying, remedying, and sanctioning (where appropriate) businesses which do not adequately comply with their obligations. We want to understand whether the framework that the Act sets up is fit-for-purpose, and whether there are any changes that could be made to ensure businesses are properly supervised and enabled to comply with their obligations.

Guiding questions for this section

- Does the Act set an appropriate foundation for effective supervision and regulation, in terms of the agencies involved and whether they have the appropriate powers and functions?
- Is there anything we could change in the Act to enable more effective supervision and regulation of businesses? Are businesses properly and adequately supported to achieve appropriate compliance with the Act?
- Are supervisors able to properly respond when businesses do not comply with their obligations? Do the available responses ensure that businesses (individually and overall) improve their compliance?

5.1. Agency supervision model

Consultation Questions

- Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it?
- If it were to change, what supervisory model do you think would be more effective in a New Zealand context?

Response

When New Zealand was in the process of drafting the AML/CFT Act and needing to consider the supervisory model, issues that had to be addressed were human resourcing and capability of developing systems to facilitate AML/CFT supervision. Given time constraints, he easier option was to absorb the role of AML/CFT supervision into existing government agencies, as opposed to creating a single standalone agency.

I previously supported the multi-armed supervisory model, however over the 7-8 years that the AML/CFT framework has been operating, I now change this view and without exception, support a single standalone agency.

Difficulties in segregating responsibilities

The AML Supervisor agencies have a number of responsibilities, other than AML Supervision. The RBNZ has responsibility for prudential oversight of our banking sector and life insurance industry. The FMA has responsibility for the oversight of our financial markets to ensure a fair and orderly market. The DIA have oversight of immigration, citizenship, passports, births deaths and marriages, gambling (and more). This creates the risk that dedicated resourcing is not being committed to AML/CFT Supervision, in favour of other, more pressing responsibilities.

Whereas the AML/CFT Act enables that AML Supervisors may use information obtained to assist their performance in other roles, the AML/CFT Act explicitly prohibits using personal information to support their other roles (s.137). There is real risk that it is too difficult or impossible to ensure the segregation of powers.

To demonstrate these concerns, the FMA does not operate with a dedicated AML/CFT team. The FMA combines the market oversight team with AML Supervision. The DIA operates with a number of law enforcement functions and I am aware at least one onsite inspection was carried out under the AML/CFT Act, but the DIA officials utilised powers of search by requesting the business employees to produce confirmation of their immigration status. These are examples of the types of problems that do arise or will arise by placing AML Supervision under the controls of agencies that have other regulatory commitments and law enforcement powers. It can lead to acts of corruption (abuse of power), either knowingly or unintended.

Standalone Agency

I strongly support the establishment of a standalone agency, built on the same model existing in Australia. Australia uses a standalone unit for both the oversight supervisory function, as well as the financial intelligence unit.

By removing the financial intelligence role away from the NZ Police and into a dedicated AML/CFT unit, this will mitigate risks arising from limited staff resourcing that occurs within the NZ Police. It removes potential conflicts between varying responsibilities that the Commissioner of Police faces.

Improving trust with stakeholders and the business community

Operating with a standalone entity would improve trust from the public that the AML/CFT supervisory model has a single commitment and is not multi-faceted.

Improve consistency of regulatory action

As an AML/CFT consultant operating prior to and since the implementation of the AML/CFT Act, I have been in a position of actively engaging with the industry and also observing Supervisory actions and outcomes.

I have become very concerned at the lack of consistency across supervisory bodies (the DIA and FMA). I have seen improper regulatory targeting and witnessed regulatory action that had no element of fairness.

Despite receiving clear and indisputable information that there were systemic risks arising within the industry causing material breaches, the DIA and FMA refused to correct those matters through guidance material or newsletters.

The actions of the DIA and FMA are being recognised across the industry as repressive and aggressive actions (refer NBR article 12 April 2021, by reporter Hamish McNicol).

AML/CFT compliance will continue to be one of the greatest weapons available to governments to try and combat organised crime. It is time that New Zealand committed a better model than the existing one and that the government dedicate resourcing to get the balance right between private and public commitments to making the AML/CFT framework succeed.

5.2. Mechanisms for ensuring consistency

Consultation Questions

- Do you think the Act appropriately ensures consistency in the application of the law between the three supervisors? If not, how could inconsistencies in the application of obligations be minimised?

- Does the Act achieve the appropriate balance between ensuring consistency and allowing supervisors to be responsive to sectoral needs? If not, what mechanisms could be included in legislation to achieve a more appropriate balance?

Response

In my role as an AML/CFT consultant and auditor, I have provided services to reporting entities and DNFBPs who collectively fall under the umbrella of the three AML Supervisors. However, predominantly my clients are supervised by the DIA.

I have seen material inconsistencies of decision making and actions within a single agency, as well as across agencies.

It is accepted that each agency are supervising very different sectors. The DIA's sector is predominantly small businesses. The FMA's sector is predominantly mature businesses who are used to dealing with regulations and the RBNZ supervise a combination of entities, including registered banks.

Though the sectors are quite different, there needs to be a level of consistency in the application or regulatory expectation. It would be unfair for one supervisor to not penalise a reporting entity who is consistently failing in customer due diligence (CDD) obligations, yet penalise another who was identified on one occasion of not meeting CDD expectations.

I have witnessed circumstances of the DIA receiving information in annual regulatory reports that the reporting entities have no risk assessment or programme in place (absolute mandatory requirements), or have not undertaken any independent audit (another mandatory requirement) – yet taken no action. This is despite the reporting entities operating in a high risk sector. No action was taken, such as writing to the reporting entity to confirm their obligations and placing the reporting entity on a follow-up risk mitigation plan.

On other occasions I have seen reporting entities operating with systems that are above the industry standard, with no material breaches and regulatory action has taken placed, based on trivial matters.

Segregated Systems

The three-pronged approach of the supervisory model results in each government agency operating with separate systems, with each system having different capabilities. If one Supervisory agency operates with a capable system and another agency does not, this creates a risk that entity's who are consisting breaching

AML/CFT laws are not identified.

Compliance Strategy

Regardless of the size of the entity, ML/FT risks exist. To ensure the consistency of supervisory oversight and regulatory actions, the three agencies should, if not already, establish a compliance strategy and agree collectively (not individually) on what types of breaches or circumstances would exist before regulatory action is taken. They also need to determine what that regulatory action may look like. Each agency will no doubt have differences of risk appetite which wouldn't be discouraged, however it would assist in trying to achieve a consistency of a proportionate and flexible approach.

Standalone Agency

By having three separate agencies working under different internal capabilities, systems and controls, it is likely the existing arrangement will always struggle to achieve a fair and consistent approach.

The best way to achieve consistency in the AML/CFT supervisory model, is to transition the existing AML Supervisory model into a singe agency.

5.3. Powers and functions

Consultation Questions

- Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why?

Response

The existing powers and functions contained in sections 131 and 132 are satisfactory in order for an AML Supervisors to achieve their regulatory objectives.

Supportive Role

AML Supervisors however are not adequately utilising these functions to understand the issues that reporting entities are facing and how the AML Supervisors may mitigate those issues, either through providing guidance or establishing a Code of Practice.

Supervisors can achieve this by carrying out thematic reviews and surveying reporting entities on the matters that are working well and the matters that are not working well.

It would have been helpful if AML Supervisors had carried out such a review leading up to this statutory review. If they had done so, they would have been better equipped to understand the issues facing the industry and been in a better position to recommend changes that may have assisted to overcome those issues.

Onsite Inspections

Onsite inspections are evasive, especially to small entities. AML Supervisors need to be more considerate in determining when an onsite visit would be required. An onsite visit to a small business, with limited human resourcing, can significantly disrupt that business and cause significant stress, especially if the conduct of the onsite inspectors is intimidatory.

Engaging Stakeholders

AML auditors provide a third line of defence to reporting entities. Auditors are also a resource relied on by AML Supervisors.

AML Supervisors should engage with a wide range of auditors more frequently. This would be another information source to assist AML Supervisors understand the issues that are being identified in the industry that are impacting upon reporting entities.

Rights of Appeal

Do AML Supervisor’s operate with an Enforcement Policy that sets out the criteria and processes that must

be applied prior to using powers of enforcement?

I am aware of one reporting entity who had regulatory action taken against them that was unjustified and disproportionate. It appeared to be unfair targeting. When the reporting entity sought to respond to the regulatory action by meeting with the decision makers to discuss the issues, they were denied that right. The regulatory simply responded their decision was made and final.

The pecuniary penalty determined the the AML Supervisor had the same result upon the reporting entity, if a court had determined the decision. The differences however is that a court allows an accused person to be presented and to defend their position. The actions by this AML Supervisor denied this right. It was unfair, unjust and unreasonable. Further enquiry found that the AML Supervisor had in fact set out on a course of action to bring a regulatory action, in advance of notifying the reporting entity. These matters are well documented and can be independently established.

This is a situation in which I am left in no doubt the reporting entity has been harassed and intimidated by the AML Supervisor without proper cause. This is not just my view but the view form others key stakeholders in the industry.

If AML Supervisors have the ability to cause severe pecuniary penalty upon a reporting entity, their regulatory power needs to be balanced with the rights of a reporting entity.

AML Supervisors need to operate with a policy that establishes a fair regulatory process, one that allows proper consideration for a response and one that enables the AML Supervisor to utilise their internal powers with a proper establishment of a regulatory committee.

Supervisors need to understand the importance of separating the executive from the judiciary and the rule of law. There should be some type of appeal process against decisions made by an AML Supervisor.

Any powers and sanctions that can be made from an AML Supervisor should be proportionate.

5.4. Regulating auditors, consultants, and agents

Independent Auditors

Consultation Questions

- Should explicit standards for audits and auditors be introduced? If so, what should those standards be and how could they be used to ensure audits are of higher quality?
- Who would be responsible for enforcing the standards of auditors?
- What impact would that have on cost for audits? What benefits would there be for businesses if we ensured higher quality audits?
- Should there be any protections for businesses which rely on audits, or liability for auditors who do not provide a satisfactory audit?

Response

Auditors are a resource that AML Supervisors significantly rely on for ensuring AML/CFT compliance standards are met. There should therefore be an alignment between the outputs of an auditor's report to the regulatory objectives that AML Supervisors seek to achieve.

AML Supervisors can achieve this by setting prescribed requirements of what must be included in an auditor's report which would prevent the situation of auditors failing to analyse matters considered material.

As an alternative to prescribing requirements, the framework could require an AML/CFT auditor to be registered. Upon registration, an introductory package could be sent to the auditor, setting out AML Supervisors' preferred approach and encouraging the auditor to make contact should they have any questions.

Collaborate

AML Supervisors recently held an auditors' forum. It was well received and encouraged discussions.

Continuing with this type of forum will enable AML Supervisors to not only better understand the issues facing the industry, but it will also allow them a means to communicate their expectations.

When auditors get it wrong

An audit used to occur every 2 years. Regulations have now changed this to every 3 years and at an AML Supervisor's discretion, this can be changed to every 4 years.

An auditor's role is to examine the operations of the programme. In practice this means an auditor could be expected to examine between 3-4 years of transactions and determine whether systems are adequate and capable of detecting suspicious activity. As most auditors use manual systems for auditing, it is not possible

for all transactions to be reviewed. Depending on the size of the business, this could mean only 1%-2% of transactions are reviewed. The same issues apply to reviewing customer onboarding. Depending on the size of the customer base, only a small portion of customer files may be examined.

If the auditor's findings that the reporting entity was compliant, but later the reporting entity faced regulatory action for a single breach of customer due diligence – should the auditor be penalised for an "unsatisfactory" audit? Of course not.

There needs to be more information provided on what would qualify an audit report being unsatisfactory. Does this mean the format or lack of in-depth analysis?

A standard for audits can be achieved through greater engagement from AML Supervisors, such as establishment of an auditors forum.

Considerations of Liability to Reporting Entities

If a reporting entity is facing regulatory action and the AML Supervisor determines the regulatory action in part was contributed to an unsatisfactory audit, there should be some level of mitigation in the regulatory penalty. Whether the reporting entity pursues those issues with the AML Auditor is for the reporting entity to determine.

Consideration of Liability to Auditors

I do not agree that the AML Supervisors should be involved in penalising auditors. There are a number of reasons for this. The first is that I have witnessed AML Supervisors network with a small number of auditors and isolate other auditors. There is clearly favouritism that exists in the current market. This is a view that is shared with other auditors and is not just my own.

I have also seen circumstances where AML Supervisors have disagreed with auditors, however a number of the issues in this statutory review confirms those issues, from the eyes of the MoJ, were indeed ambiguous.

AML Supervisors do not like to be challenged. If auditors do their job well and along the way upset AML Supervisors, this may lead to disproportionate regulatory action against those auditors.

Ensuring a Competitive Market

AML/CFT compliance is always intended to have proportionate costs for the industry. Small businesses cannot afford the costs of an AML/CFT audit from larger institutions. The cost competitive environment should be something that AML Supervisors encourage – so long as the auditing process and outputs are reasonable and meeting industry expectation.

Providing a regulatory framework that penalises AML/CFT auditors may discourage small auditing firms from operating in the market. This would cause audit costs to considerably rise.

Recommendations

To encourage and monitor auditing standards, the following recommendations are made:

- AML Supervisors create a system requiring AML/CFT auditors to register.
- Upon registration the auditor receives a ‘welcoming package’, incorporating the auditing guidelines and other material that assists AML Supervisors to provide an industry standard and expectation.
- AML Supervisors promote an auditors forum, allowing any industry issues of concern to be addressed.

Consultants

Consultation Questions

- Is it appropriate to specify the role of a consultant in legislation, including what obligations they should have? If so, what are appropriate obligations for consultants?
- Do we need to specify what standards consultants should be held to? If so, what would it look like? Would it include specific standards that must be met before providing advice?
- Who would be responsible for enforcing the standard of consultants?

Response

Most auditors in the industry also act as consultants and advisory experts to reporting entities.

The industry is common with the term ‘consultant’ and it should not need any clarification in legislation.

The same responses provided under the consultation questions relating to Auditors applies to this consultation query relating to Consultants.

If the AML Supervisors are concerned about quality of advice, they have the ability to provide newsletters or guidelines on what issues reporting entities should consider before engaging a consultant. The obvious is that the reporting entity should check the level of experience of the consultant and whether they hold any specialist qualifications in the AML/CFT field.

As it is the role for consultants to at times justly challenge an AML Supervisors finding, it may lead to AML Supervisors targeting consultants, utilising the regulatory power they hold.

Stakeholders, such as consultants, represent their client. It should be the client that determines the qualities they seek in a consultant, not a prescribed standard set by AML Supervisors.

By prescribing standards and penalties that impact on the consulting industry, the risk is that AML Supervisors create a situation that impedes a competitive market. AML Supervisors should therefore be dissuaded from having wide and arbitrary powers over the industry.

5.5. Comprehensiveness of Regulatory Regime

Consultation Document

- Another option could be to allow AML/CFT supervisors to impose administrative penalties, such as restricting, suspending, or withdrawing a business's license or registration for non-compliance with AML/CFT obligations.

- Such tools may be used for low level compliance breaches that are not serious enough to warrant injunctions or court imposed pecuniary penalty and where the misconduct does not result in serious harm or involve complex situations.

Response

This consultation query is proposing that AML Supervisors be authorised to take severe pecuniary penalty, such as closing down a business which causes loss of employment and financial hardship, based on "*low level compliance breaches*" that are "*not serious enough to warrant a court imposed pecuniary penalty*".

If the conduct of concern is low level and not serious enough to warrant a court penalty – why would an AML Supervisor consider that causing severe stress, financial hardship and loss of employment is ok? This is ludicrous and is of concern that AML Supervisors and/or the MoJ could even suggest such a desire. Penalties should be proportionate. If the offending is 'low level', it would not justify the closure of a business. If the MoJ and AML Supervisors consider such an action would be reasonable, then it is clear they do not have the business community's best interests in mind.

AML Supervisors need to establish and publish an enforcement framework. The framework needs to incorporate processes that are fair, just and ensure any accused party is afforded an opportunity to defend.

My experience to date are that the DIA and FMA are yet to establish an adequate supervisory framework to ensure their powers are used proportionally. Providing greater powers arising from this statutory review has a real risk of harming the reputation NZ's AML/CFT framework.

Before regulatory powers are increased, the DIA and FMA need to establish they operate are a framework that is considered adequate, fair and just to the wider business community.

Providing powers to government to issue pecuniary penalty and avoiding an independent judicial framework such as a court of law, increases the risk that their internal powers will be used outside the principles of the rule of law.

6. Liquidation following non-payment of AML/CFT Penalties

Consultation Question

- Should DIA have the power to apply to a court to liquidate a business to recover penalties and costs obtained in proceedings undertaken under the Act?

Response

The consultation document has not confirmed if recovery of pecuniary penalties is limited to penalties resulting from a court action or whether the intention is to incorporate the ability to recover penalties resulting from DIA's self-imposed penalty action.

If it is the latter then no – such power is not warranted. Penalties arising from a court action have greater separation between the recovery action.

7. Information that needs to be reviewed for account monitoring

Consultation Question

- Should we issue regulations requiring businesses to review other information where appropriate as part of account monitoring? If so, what information should regulations require businesses to regularly review?

Response

Suggestion is too prescriptive and may remove or discourages reporting entities to use innovative monitoring techniques that are more effective.

Stipulating monitoring techniques will likely increase compliance costs.

A better suggestion is for AML Supervisors to use guidelines.

An IP address is not a reliable monitoring technique. IP addresses can be manipulated through VPN plugins.

FATF's Mutual Evaluation Report 2021 indicates the FIU are not using sophisticated systems. The report provides information to show the FIU are relying on keywords searches and are only analysing 20% of suspicious activity reports received.

Enabling the ability for the FIU or AML Supervisors to prescribe techniques for monitoring has the risk of pushing obligations for detection disproportionately to the private industry.

8. Conducting CDD on existing (pre-Act) customers

Changing ‘and’ to ‘or’ is reverting back to what the original Bill had set out to achieve.

I agree that correcting this anomaly is required.