

Review of the AML/CFT Act

Consultation Document

Ministry of Justice

October 2021



MINISTRY OF
JUSTICE
Tabu o te Ture

New Zealand Government



Important notice

The opinions contained in this document are those of the Ministry of Justice and do not reflect official government policy. Readers are advised to seek specific legal advice from a qualified professional person before undertaking any action in reliance on the contents of this publication. The contents of this discussion document must not be construed as legal advice. The Ministry does not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken as a result of reading, or reliance placed on the Ministry because of having read, any part, or all, of the information in this discussion document or for any error, inadequacy, deficiency, flaw in or omission from the discussion document.

Contents

| | |
|--|-----------|
| Glossary of terms..... | i |
| Introduction | ii |
| About this document | viii |
| How to make a submission | xi |
| Institutional arrangements and stewardship..... | 1 |
| Purpose of the AML/CFT Act | 1 |
| Risk-based approach to regulation..... | 4 |
| Mitigating unintended consequences | 7 |
| The role of the private sector | 8 |
| Powers and functions of AML/CFT agencies | 9 |
| Secondary legislation making powers | 12 |
| Information sharing | 14 |
| Licensing and registration | 15 |
| Scope of the AML/CFT Act..... | 19 |
| Challenges with existing terminology | 19 |
| Potential new activities..... | 25 |
| Currently exempt sectors or activities | 30 |
| Potential new regulatory exemptions | 32 |
| Territorial scope | 34 |
| Supervision, regulation, and enforcement | 37 |
| Agency supervision model | 37 |
| Powers and functions..... | 39 |
| Regulating auditors, consultants, and agents..... | 40 |
| Offences and penalties | 42 |
| Preventive measures..... | 47 |
| Customer due diligence | 47 |
| Record keeping..... | 66 |
| Politically exposed persons..... | 67 |
| Implementation of targeted financial sanctions | 72 |
| Correspondent banking..... | 76 |
| Money or value transfer service providers..... | 77 |
| New technologies | 79 |
| Virtual asset service provider obligations | 81 |

| | |
|--|------------|
| Wire transfers | 82 |
| Prescribed transaction reports | 86 |
| Reliance on third parties | 90 |
| Internal policies, procedures, and controls | 93 |
| Higher-risk countries | 96 |
| Suspicious activity reporting..... | 98 |
| High value dealer obligations | 100 |
| Other issues or topics..... | 103 |
| Cross-border transportation of cash..... | 103 |
| Privacy and protection of information | 105 |
| Harnessing technology to improve regulatory effectiveness..... | 106 |
| Harmonisation with Australian regulation | 108 |
| Ensuring system resilience | 108 |
| Minor changes | 109 |
| Definitions and terminology..... | 109 |
| Information sharing | 110 |
| SARs and PTRs..... | 110 |
| Exemptions..... | 111 |
| Offences and penalties | 112 |
| Preventive Measures | 112 |
| Index of terms..... | 114 |

Glossary of terms

| | |
|----------------------------|---|
| 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 Act |
| CDD | Customer Due Diligence |
| DBG | Designated Business Group |
| DIA | The 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 |
| VASPs | Virtual Asset Service Providers |

Introduction

New Zealand's *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009* (the Act) is a core part of our effort to detect and deter money laundering and terrorism financing.

To put it simply, money laundering and terrorism financing are crimes. Money laundering is the process criminals use to 'clean' the money they make from crimes such as fraud, dealing in illegal drugs, tax evasion and trafficking. By making the money look like it comes from a legitimate source, criminals can cover their tracks and avoid detection. Criminal organisations and people who finance terrorism target businesses and countries they believe have weak systems and controls they can exploit.

Money laundering is happening every day across New Zealand. The Financial Intelligence Unit estimated that over \$1 billion a year of dirty money comes from drug dealing and fraud which may be laundered through New Zealand businesses. However, the true cost and impact is many times that figure when you factor in all the crimes that generate "dirty" money and the suffering they cause. People who finance terrorism also use these methods to send money to violent causes and to disguise who is providing and receiving the money. While the likelihood of terrorism financing is low, the potential consequences are significant.

Our Act makes it harder for criminals to launder money and provides a significant disincentive to carrying out the criminal activity in the first place. The Act requires businesses to, among other things, check customer's identification, monitor accounts for suspicious activity, and report suspected money laundering and terrorism financing to the New Zealand Police. As a result, the Act also make New Zealand less attractive as a destination of international money laundering and offending and reduce the ability for terrorism to be financed through our businesses.

However, these protections come at a significant cost, primarily to the approximately 10,000 businesses who have some exposure to money laundering and terrorism financing risks. These businesses have been required to comply with the AML/CFT regime for a number of years and have faced an increased cost of doing businesses and other restrictions with how they can operate. The regime has also made it harder, if not impossible, for some people and businesses to get access to basic banking services and participate in the economy.

A review commenced on 1 July 2021

The Minister of Justice, Hon Kris Faafoi, commenced a review of the AML/CFT Act on 1 July 2021. This review is an opportunity to look back on the past eight years and ask ourselves: have we got this right? Does the regime effectively achieve its purposes in the most cost-efficient way? What can we do better? What can we do without?

The review is being led by Te Tāhū o Te Ture, the Ministry of Justice. However, we are supported in this process by the other government agencies which have roles and responsibilities in the AML/CFT regime, specifically Department of Internal Affairs, Financial Markets Authority, New Zealand Customs Service, New Zealand Police, and Reserve Bank of New Zealand. The Ministry has also established an Industry Advisory Group to provide additional guidance and support as we conduct the review.

We have developed Terms of Reference for the review, which are available here: www.justice.govt.nz/amlcft-review. These Terms set out our aspirations for the review, which is that New Zealand becomes the hardest place in the world for money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction. In doing so, the AML/CFT regime will help maintain a safe, trusted, and legitimate economy.

Our review will be guided by a series of principles, which we will use to inform what recommendations we eventually make. These principles are to:

- create a financial environment which is hostile to serious and organised crime and national security threats;
- appropriately and responsibly manage the risks we are exposed to through clear obligations on businesses, agencies, and the public;
- ensure agencies have proportionate and appropriate powers and functions;
- facilitate support and enhance domestic and international collaboration and cooperation;
- adopt international best practices where appropriate to ensure New Zealand fulfils its international obligations and addresses matters of international concern;
- work in cooperation with industry, public, and Māori and other impacted communities;
- ensure the AML/CFT regime produces the necessary type and quality of information to support other frameworks and to combat money laundering, terrorism financing, and serious and organised crime;
- ensure that human rights and privacy considerations are addressed and that intrusions on personal rights and freedoms are no more than necessary; and
- support efficient long-term administration of the regime.

Ultimately, we see this review as start of a conversation about how we can make our AML/CFT regime the best it can be. We want an AML/CFT regime that maintains New Zealand's status as having a high quality and effective regime for combatting money laundering and terrorism financing without compromising the ease of doing business or unduly impacting the lives of New Zealanders. We also want to make sure the regime contains sufficient tools to enable flexibility and ensure the regime responds to changing risks and new opportunities for addressing harm.

Scope of the review

This review is required by [section 156A](#) of the Act and requires two questions to be answered: how has the Act has operated and performed since 2017; and what in the Act can or should change? Answering these two questions requires the Ministry to review the Act and other instruments (such as regulations and Codes of Practice) to understand how they have performed and whether they continue to be fit-for-purpose.

The following is within scope of the review:

| Instrument | Description |
|---|---|
| <u>AML/CFT Act 2009</u> | Principal AML/CFT legislation. |
| Regulations issued under the AML/CFT Act, namely: <ul style="list-style-type: none"> - <u>AML/CFT (Cross-Border Transportation of Cash) Regulations 2010</u>; - <u>AML/CFT (Definitions) Regulations 2011</u>; - <u>AML/CFT (Exemptions) Regulations 2011</u>; - <u>AML/CFT (Ministerial Exemption Form) Regulations 2011</u>; - <u>AML/CFT (Prescribed Transactions Reporting) Regulations 2016</u>, and - <u>AML/CFT (Requirements and Compliance) Regulations 2011</u> | These regulations have been issued using the regulation making powers in the Act. They provide further detail about who is and who is not captured by the regime, set out additional steps businesses are required to do to comply, and describe how various reports need to be made under the Act. |
| The various class exemptions contained in the <u>AML/CFT (Class Exemptions) Notice 2018</u> | This instrument sets out 15 exemptions for classes of businesses or transactions issued by the Minister of Justice. |
| <u>Amended Identity Verification Code of Practice 2013</u> | This instrument sets out suggested best practice for how businesses can conduct name and date of birth verification for low and medium risk customers. |

The content of any guidance issued by the AML/CFT supervisors or by the New Zealand Police is not within scope of the review, nor is the substance of any individual exemption issued by the Minister of Justice. However, the role that guidance and exemptions play in achieving the purpose of the regime is within scope.

The AML/CFT regime intersects with a number of other pieces of legislation and regulation, for example the *Crimes Act 1961*, *Terrorism Suppression Act 2002*, *Companies Act 1993*, and the *Trusts Act 2019*. Considering changes to other legislation is not within scope of this review, despite their relevance to the operation of the overall AML/CFT regime.

Why we might recommend changes

In line with the guiding principles of the review, there are several reasons why we might ultimately recommend changes to the Act or various AML/CFT instruments. Forming a recommendation will involve a careful balancing of the need to address the harms of money laundering and terrorism financing while ensuring that businesses can operate efficiently and innovatively.

Addressing emerging areas of risk and supporting other government priorities

The AML/CFT system needs to be responsive to new and emerging risks or concerns. Some issues have been identified because we know they are likely being used for money laundering and terrorism financing, while other we have identified other issues because they are vulnerable

to misuse. Further, some areas of risk may also be a global concern (e.g. virtual assets), while other risks are more particular to New Zealand (e.g. trust and company service providers).

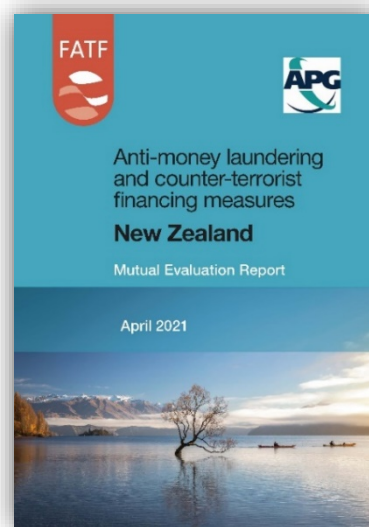
The Government has agreed to several programmes of work and strategies where the AML/CFT regime could play a role. For example, in 2019, Cabinet agreed to the *Transnational Organised Crime Strategy* to prevent, detect and dismantle organised crime in a unified manner. Money laundering is a key enabler of organised crime and strengthening our regime could help to achieve these policy objectives. The same is true for combatting cybercrime as part of New Zealand's *Cyber Security Strategy 2019*, as many cybercrimes are profit-motivated.

Improving compliance with Financial Action Task Force standards following our Mutual Evaluation

Our AML/CFT regime is part of a worldwide system to tackle money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction. New Zealand is a member of the Financial Action Task Force (FATF), an inter-governmental body that sets relevant standards (FATF Recommendations) with which all countries are required to comply.

New Zealand's AML/CFT system is periodically peer reviewed by other FATF members through a process known as a Mutual Evaluation. A Mutual Evaluation provides an in-depth assessment of how effective a country's system is and the extent to which it complies with the FATF standards. Mutual Evaluations can also provide focused recommendations to the country to further strengthen its system.

New Zealand was recently evaluated by the FATF and we have a clear roadmap for how we can improve our regime and continue to keep New Zealand safe. The FATF has identified where our laws do not comply with their standards and provided several recommendations for how we can improve our effectiveness. These deficiencies and recommendations are a key driver for change, but we will also consider whether relevant recommendation is appropriate in New Zealand's risk and context.



New Zealand's Mutual Evaluation

Where the FATF's standards, findings or recommendations are relevant to the topic at hand, we will use this style of text box to pull out the relevant information from our Mutual Evaluation or the FATF standards.

Ensuring compliance costs are proportionate to risks for our economy

We also want to ensure that compliance costs are proportionate to risks for individual businesses and across the economy in general. Our law might fully or mostly meet the FATF's standards, but that does not mean that the obligation is straightforward for businesses or that it provides as much value as it could. There are often many ways we can achieve the outcomes of the Act, and we may not have chosen the most efficient option at the time we developed the obligation. As the system has matured, businesses also may have identified better or more efficient ways of doing

things that ultimately reduce compliance costs overall. We are interested in hearing about better and more innovative ways to for the system to work.

Another related consideration is the size and nature of our economy. New Zealand is a relatively small developed economy, with many businesses being subsidiaries of offshore parent businesses. Businesses may also provide a more general service which can be provided by specialist businesses in other, larger economies. We also may be more reliant on overseas investors and businesses to offer services in New Zealand, which may impact how willing businesses are to compromise on the ease of doing business.

Modernising the Act and our approach to reflect the digital economy

The past decade has seen a paradigm shift for many towards the digital economy, and this shift is relevant to the development and operation of the entire regime. We live in a very different world than we did in 2009 when the Act was being developed, and many New Zealanders now live far from their nearest physical branch, and generally engage with businesses mostly or entirely online. This trend is only set to accelerate with the increased availability of online communication tools and postal services and other traditional communication tools are becoming less available or reliable. Further, many services are provided by overseas businesses with no presence in New Zealand at all. We want to ensure the AML/CFT regime is able to work properly in 2021 and that it reflects how the digital economy operates and is future-proofed (to the extent this is possible).

Avoiding or mitigating unintended consequences

While the AML/CFT regime aims to ultimately protect communities from harm, there are many people who may be inadvertently harmed by its operation. The misapplication of AML/CFT measures can have serious negative effects, including suppressing legitimate non-profit organisations, de-risking, financial exclusion, and restriction of fundamental human rights. This issue is not unique to New Zealand: internationally, the FATF has recognised several areas where implementing AML/CFT has undermined other policy objectives. While we have identified some areas where our regime may have unintended and harmful consequences (see page 7), we are aware that there could be more. We want to ensure that any unintended consequences are reduced, if not entirely avoided.

Next steps following the statutory review

The review will finish by 30 June 2022 with the Ministry providing a report to the Minister of Justice that outlines how the Act has performed since 2017 and recommends any changes that could be made to the Act. From there, the Minister is required to table the Ministry's report in the House of Representatives, at which point the report will become public.

It can take at least two to three years to implementing legislative changes to address any recommendations we make. This would require the government to design the changes, introduce a new Bill into the House of Representatives, and for the Bill to be passed into law.

Earlier changes may be made through secondary legislation

The Act allows for a wide variety of changes to be made through "delegated legislation" or "secondary legislation". The Act allows for:

- **the Governor-General to issue regulations** on the recommendation of the Minister of Justice under [sections 153](#), [154](#), and [155](#). These can be used to prescribe requirements

for various obligations such as customer due diligence, including and excluding types of businesses, and imposing countermeasures against high-risk countries.

- **the Minister of Justice to issue exemptions** using [section 157](#) to exempt classes of businesses and transactions from some or all of the Act. Exemptions must expire after five years.
- **the Ministers responsible for the AML/CFT supervisors to issue Codes of Practice** under [section 64](#) which can provide businesses with a safe harbour for how to comply with their obligations under the Act.

These powers could allow us to progress some changes and enhancements at an earlier stage without changing the Act. Taking this approach would ensure pain points, challenges, and enhancements are made as soon as possible. It could also enable us to improve New Zealand's compliance with the FATF's standards at an early stage and allow us to exit the FATF's resource-intensive "enhanced follow up process." However, we would only look to make relatively straightforward changes that address discrete issues that would not be impacted by later legislative changes.

We intend to provide advice to Minister Faafoi in early 2022 on changes that could be made at an earlier stage through secondary legislation.

Timeframes for the review

The review will proceed along the following indicative timeframe:

| Stage | Timeframe |
|--|------------------------|
| Public consultation closes | 3 December 2021 |
| Further targeted consultation with private sector and communities to form recommendations | February to April 2022 |
| Advice provided to Minister Faafoi on earlier regulatory changes | April 2022 |
| Report provided to Minister Faafoi, to be tabled in the House of Representatives as soon as practicable thereafter | 30 June 2022 |

About this document

This document has been developed based on what we and the other AML/CFT agencies have identified as areas of concern. We want to be transparent and consult on these topics to ensure we have a robust discussion about the future of our AML/CFT regime. However, we recognise that there are likely to be issues or changes that we have not identified and want to hear all suggestions you may have (some guiding questions are provided below).

We have structured these issues into six parts, with a number of sub-topics for you to consider. The six parts are:

1. **Institutional arrangements and stewardship:** are the foundations of our AML/CFT regime correct? Does the regime have the correct purposes? Is the regime set up in a way that ensures it is flexible and responsive?
2. **Scope of the AML/CFT Act:** do the right businesses have AML/CFT obligations, given New Zealand's risks? Do those businesses have the right obligations?
3. **Supervision, regulation, and enforcement:** is the supervision framework appropriate? Do we need additional or supplementary regulation to ensure businesses are protected from harm? Is there a sufficient penalty framework to ensure that proportionate and effective sanctions can be imposed?
4. **Preventive measures:** are AML/CFT obligations, such as customer due diligence, sufficient to prevent businesses from being misused for money laundering or terrorism financing? Are they able to be implemented efficiently to avoid unnecessarily large compliance burdens for businesses?
5. **Other issues or topics:** is the border cash reporting regime fit-for-purpose for New Zealand to prevent cross-border movements of illicit funds? Have we appropriately considered other issues, such as privacy concerns, the ability to use technology to improve outcomes, and harmonisation with Australian regulation?
6. **Minor changes for clarity:** what small tweaks can we make to address issues or improve clarity?

Areas of potential focus

This document has been written with a primarily technical audience in mind, as we anticipate that businesses with AML/CFT obligations will be most interested in the review.



We have also produced a summary document which provides a high-level overview of the issues we are consulting on. You can access this document at www.justice.govt.nz/amlcft-review.

All respondents are likely to be interested in Part 1, as the part engages with the fundamentals of our AML/CFT regime. All businesses involved in the AML/CFT regime will be interested in Part 3, relating to supervision and enforcement of the Act, and aspects of Part 4 that apply to all businesses (Customer due diligence, Record keeping, Politically exposed persons, Implementation of targeted financial sanctions, New technologies, Reliance on third parties, Internal policies, procedures, and controls, and Suspicious activity reporting).

However, depending the nature of your business, you may be especially interested in the following areas:

| Business type | Areas of interest |
|--|---|
| Financial institutions | <ul style="list-style-type: none"> • Definition of financial institution activities (page 22); • Businesses providing multiple types of activities (page 20); • Overlap between “managing client funds” and financial institution activities (page 21); |
| Insurers | <ul style="list-style-type: none"> • Non-life insurance businesses (page 26); • CDD on beneficiaries of life and other investment related insurance (page 53) |
| DNFBPs | <ul style="list-style-type: none"> • “In the ordinary course of business” (page 19); • “Managing client funds” (page 21), the overlap between “managing client funds” and financial institution activities (page 21), and CDD obligations when managing funds in trust accounts (page 51); • “Engaging in or giving instructions” (page 22); • Acting as a secretary of a company or partner in a partnership (page 25); • Criminal defence lawyers (page 26) and protections for legally privileged information (page 106); • Combatting trade-based money laundering (page 28); • Exemption for acting as trustee or nominee (page 32); • Definition of a customer in real estate transactions (page 49); |
| Remitters | <ul style="list-style-type: none"> • De-risking (page 7), the use of agents (page 42), money or value transfer service provider obligations (page 77), wire transfers (page 82) and prescribed transaction reports (page 86), and SAR obligations for remitters (page 100) |
| High value dealers | <ul style="list-style-type: none"> • Definition of “high value dealer” (page 23), high value dealer obligations (page 100), appropriate cash transaction threshold (page 24) and threshold for PTRs (page 89). • Exemption for pawnbrokers (page 23) |
| Virtual asset service providers | <ul style="list-style-type: none"> • Including all types of Virtual Asset Service Providers (page 27) • Virtual asset service provider obligations (page 81) |
| Businesses with international exposure | <ul style="list-style-type: none"> • Territorial scope (page 34) • Politically exposed persons (page 67) • Correspondent banking (page 76); • Wire transfers (page 82) and prescribed transaction reports (page 86) • Group-wide programme requirements (page 94) • Higher risk countries (page 96) |

We are asking two types of questions

In each section or topic, we ask a series of questions to obtain the feedback we are particularly interested in. However, just because we are asking a question about a potential change or issue does not mean that we will ultimately recommend that the change happen. You also do not need to be constrained by the questions we have asked, and you can answer as many or as few questions as you like.

We ask two types of questions throughout the document, depending on whether we think the issue or topic could potentially be addressed at an earlier stage using the secondary legislation making powers in the Act. We differentiate between these questions as follows:



We will use this style of question box to denote questions relating to issues that **require longer term and substantive work, and likely require legislative changes**. These questions tend to be more high-level, open ended and reflect that the fact that we are generally at an earlier stage in the policy process, but some questions relate to specific options we have already identified.

We will use this style of question box to denote questions relating to issues that could be **addressed at an earlier stage through secondary legislation**. These questions tend to be more specific, targeted, and focused on potential options for changes we have identified. We are interested in your views about whether we should make the change, your preferred option or options, and the impact that such a change would have on your business and how it operates.



Overall questions for the review

Some overall questions you may wish to comment on include:

- How is the Act operating? Is it achieving its purposes? Are there any areas of risk that the Act does not appropriately deal with?
- What is working and what is not? Are there areas that are particularly challenging or costly to comply with? How could we alleviate some of those costs while also ensuring the effectiveness of the system?
- What could we do to improve the operation of the Act?
- Is there anything we need to do to “future proof” the Act and ensure it can respond to the modern and largely digital economy?

How to make a submission

There are a number of ways you can provide a submission as part of this consultation process. You can:

- read about the proposals and give your feedback online at justice.govt.nz/Amlcft-review
- download and read the consultation document and either:
 - email a submission to aml@justice.govt.nz
 - post a written submission to the AML/CFT Act consultation team, Ministry of Justice, DX Box SX 10088, Wellington, New Zealand

Please send us your views by **5pm, Friday 3 December 2021**. However, if you need more time to provide feedback, please let us know as soon as possible as we may be able to accommodate this.

Personal information and confidentiality

We will hold your personal information in accordance with the *Privacy Act 2020*. The *Privacy Act 2020* establishes certain principles with respect to the collection, use and disclosure of information about individuals by various agencies, including the Ministry. Any personal information you supply to the Ministry in the course of making a submission will only be used for the purpose of assisting in the development of policy advice in relation to this review.

We intend to publish submissions that we receive on the Ministry's website with personal information redacted, but we also accept submissions made in confidence or anonymously. Please clearly indicate in the cover letter or email accompanying your submission if you do not wish for your submission, name, or any other personal information to be published on the Ministry's website or included in any summary of submissions.

We may be asked to release submissions in accordance with the *Official Information Act 1982* and the *Privacy Act 2020*. These laws have provisions to protect sensitive information given in confidence, but we cannot guarantee all information will be withheld. We will not release individual's contact details and may withhold confidential submissions if it may prejudice people's ability to provide further confidential information.

Institutional arrangements and stewardship

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.

Guiding questions for this section:

- 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?

Purpose of the AML/CFT Act

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.



- 1.1. Are the purposes of the Act still appropriate for New Zealand's AML/CFT regime or should they be changed? Are there any other purposes that should be included other than what is mentioned?

Actively preventing money laundering and terrorism financing

Increasingly, some countries and businesses have been considering whether more needs to be done to *prevent* money laundering or terrorism financing from occurring in the first place, rather than simply deterring or detecting it. However, there is no international consensus on the extent to which countries should be trying to prevent money laundering or terrorism financing.

A 'prevention' focus would require the regime to do more to actively stop money laundering and terrorism financing rather than passively deterring it. Including this purpose would also require careful consideration as to how obligations for businesses are impacted. For example, a prevention focus could mean that businesses are expected to actively stop transactions going through when there is a suspicion of money laundering or terrorism financing, rather than just reporting those transactions. We would also need to ensure that a prevention focus does not exacerbate existing unintended consequences of the regime such as de-risking and financial exclusion (discussed below at page 7).



- 1.2. 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?
- 1.3. If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there need to be any additional or updated obligations for businesses?

Combatting proliferation financing

The proliferation of weapons of mass destruction is a global concern and a significant threat to international peace and security. The UN has sanctioned the Democratic People's Republic of Korea and Iran for their efforts in obtaining weapons of mass destruction, but individuals or groups could also seek to obtain weapons of mass destruction.

Combating proliferation financing is increasingly becoming part of the FATF standards and international expectations. For example, the FATF now requires countries and businesses to identify, assess, and understand the proliferation financing risks they face to better combat attempts to finance the proliferation of weapons of mass destruction. This additional step was taken to further strengthen UN requirements to implement proliferation financing related targeted financial sanctions (discussed below) by ensuring that businesses are aware of the risks they are exposed to and do not unwittingly support or become part of proliferation financing networks or schemes.¹

However, the Act does not have an explicit purpose of combatting proliferation financing, meaning that it cannot currently be used to support New Zealand's efforts to combat proliferation financing. For example, the Act cannot require businesses to assess their proliferation financing risks and implement appropriate mitigations without having an explicit purpose of combatting proliferation financing. We also need to consider whether we are focused on addressing proliferation financing more generally, or specifically from Iran and the Democratic People's Republic of Korea.



- 1.4. 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?

¹ <https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html>

- 1.5. If so, should the purpose be limited to proliferation financing risks emanating from Iran and the Democratic People's Republic of Korea or should the purpose be to combat proliferation financing more generally? Why?

Supporting the implementation of targeted financial sanctions

Targeted financial sanctions (TFS) are a key mechanism in the fight against terrorism and proliferation of weapons of mass destruction. We want to explore whether the purpose of the Act should be expanded to allow the regime to be leveraged to support businesses with implementing their existing TFS obligations.

The UN requires countries to put in place measures to prevent designated terrorists' access to funds and other property and prohibit anyone from providing designated persons with anything further once they have been designated.² The UN also requires countries to implement TFS to prevent, suppress, and disrupt the proliferation of weapons of mass destruction by Democratic People's Republic of Korea and Iran.³ We fulfil UN requirements by designating entities as terrorist entities under the *Terrorism Suppression Act 2002* and automatically incorporating UN designations into our law. We also implement proliferation financing related TFS through regulations issued under the *United Nations Act 1946*.

The Act does not explicitly have the purpose of supporting the implementation terrorism or proliferation financing related TFS. However, the purpose is implicitly included as designations are a key tool in deterring and preventing terrorism financing, and the FATF standards set out how countries can effectively implement TFS to combat terrorism and proliferation financing. Explicitly stating that a purpose of the Act is to support the implementation of TFS would enable the Act to be properly leveraged to support businesses in implementing their obligations under the *Terrorism Suppression Act 2002* and *United Nations Act 1946*.



Expanding the Act's purpose to support the implementation of targeted financial sanctions would likely have some flow-on impacts in terms of whether businesses had specific obligations in the Act (see pages 72 to 76) and whether they were supervised for those obligations by AML/CFT supervisors (see page 11).



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

² United Nations Security Council Resolutions (UNSCR) 1267/1989 and 1988 require countries to do this for persons designated by the United Nations as being associated with Al-Qaida, ISIS (Da'esh), or the Taliban. Similarly, UNSCR 1373 requires countries to do the same for persons they designate domestically.

³ UNSCR 1718 (2005) and successor resolutions set out the relevant sanctions against the Democratic People's Republic of Korea, while UNSCR 2231 (2015) and successor resolutions set out the sanctions against Iran.

Risk-based approach to regulation

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.

Understanding our risks

We have assessed our risks in various ways: international bodies, such as the FATF, publish reports on global or regional risks; the FIU has assessed New Zealand's overall risks and publishes [National Risk Assessments](#); the AML/CFT supervisors have assessed their sectoral risks; and businesses are required to understand their own risks ([section 58](#)). These assessments are informed by one another and create a feedback loop that ensures that we have a good understanding of where our risks lie. However, we want to explore whether there are any improvements that can be made to this framework, including whether we should improve the follow of information between businesses and the government.



- 1.7. What could be improved about New Zealand's framework for sharing information to manage risks?
- 1.8. 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?

Balancing prescription with risk-based obligations

New Zealand does not implement a pure risk-based approach where the extent of a business' obligations is entirely in line with the risks they face. In some areas, our law prescribes minimum standards with which all businesses have to comply, irrespective of the risks the business is exposed to or the nature of the particular customer or transaction.

Some obligations, such as obligations for suspicious activity reporting, are required by FATF standards to be tightly prescribed. Other obligations have been prescribed to reduce uncertainty when the AML/CFT regime came into effect. However, a prescriptive approach conflicts with and limits the extent to which businesses can take a risk-based approach to complying with their obligations. In addition, businesses may also conclude that complying with the obligation to the extent it is prescribed will entirely address the relevant risks, when more is actually required.



- 1.9. 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?
- 1.10. Do some obligations require the government to set minimum standards? How could this be done? What role should guidance play in providing further clarity?
- 1.11. Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?

Capacity of smaller and larger reporting entities

It can sometimes be difficult to reflect the size and capacity of businesses within AML/CFT regimes when developing regulations, and we want to ensure that we have the right balance. New Zealand businesses with AML/CFT obligations range from large multi-national corporations to sole business operators with no additional resource. Most businesses tend to be smaller in nature and have small number of employees or lower annual turnover. In addition, larger businesses that provide a range of services broad customer base are likely to have different risks compared to smaller businesses. Larger reporting entities will likely need to have more complex AML/CFT measures and use more resource to comply with their obligations than smaller entities.



- 1.12. Does the Act appropriately reflect the size and capacity of the businesses within the AML/CFT regime? Why or why not?
- 1.13. 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?

Applying for exemptions from the Act

Section 157 of the Act allows the Minister of Justice to wholly or partially exempt businesses or classes of businesses and transactions from AML/CFT obligations.⁴ The Minister must consider the factors in section 157(3), which include the intent and purpose of the Act, the risk associated with the business, and the level of regulatory burden, whether other reporting entities would be advantaged or disadvantaged, that would exist in the absence of an exemption.

The purpose of these provisions is to allow low-risk businesses to seek relief from various obligations and ensure that their regulatory burden is proportionate to risks to which they are exposed. Businesses which are very low risk may be able to apply to be wholly exempt from the Act, while other businesses may only apply to exempt from specific obligations. Ministerial exemptions can be made for a maximum of five years and can be imposed with conditions.

New Zealand has granted approximately 120 individual exemptions, 33 exemptions for classes of businesses, transactions, or services, and issued regulations to declare 11 types of business not to be reporting entities for the purposes of the Act. Some of our exemptions drew criticism from the FATF for being granted in instances where we had not demonstrated low risks.

Chapter 2, Key Finding (d) and Recommended Action (e) (pages 31-32)

New Zealand has granted a large number of exemptions and allows for simplified measures in specific, justified circumstances. It is not clear that all the exemptions granted were in cases of proven low ML/TF risks in strictly limited and justified circumstances (certain limited and historical exemptions in relation to certain special remittance facilities, providers of some family trusts and pawnbrokers). In line with its risk understanding, New Zealand also requires enhanced measures in certain circumstances.

⁴ Businesses can also be exempt by regulations issued by the Governor-General using section 154.

New Zealand should review its exemption regime, particularly historical and transitional exemptions granted when the AML/CFT Act was introduced, to ensure that the exemptions take place strictly on the basis of proven low risk of ML/TF.

The ability for the Minister of Justice to issue exemptions ensures the regime is flexible and allows businesses which are low risk to avoid the compliance costs of the regime. However, not all countries allow for exemptions in the way our Act does. For example, the United States and Canada do not allow for individual businesses to be exempt from their AML/CFT obligations, while Australia and the United Kingdom do. We could remove the ability for Ministerial exemptions to be issued if overall there is limited value, and instead use regulations to provide relief to categories of businesses which are low risk. However, regulations would not be able to be tailored to specific businesses.

We also have identified other areas with the exemptions process that should be reviewed:

- the decision maker is the Minister of Justice. Exemptions under other regimes in New Zealand and in other countries can be made by an operational decision maker, such as the head of a government department. Changing the decision maker could make exemptions more efficient, but we would need to ensure that decisions are still being made consistently and likely by a single decision maker (e.g. the Secretary of Justice).
- although the risk of money laundering or terrorism financing associated with the business is considered when the Minister decides to grant or decline an exemption, this factor is one of several listed in the Act. Exemptions should only be granted when it can be demonstrated that the proposed exemption is low risk. In addition, it is unclear what “risk” needs to be low, i.e. the business’ risk or the risk of granting the business an exemption.
- the Act does not make it clear that the other factors (e.g. the business’ compliance burden, whether there are any competitive advantages or disadvantages if an exemption was or was not granted) are only considered once low money laundering and terrorism financing risks are not themselves grounds for an exemption.
- the amount or quality of information that applicants should provide when applying for or renewing exemptions is unspecified, which can result in applications lacking the required detail to be properly assessed. Requiring applicants to prove they are low risk when applying could make processing exemptions more efficient, but would increase the burden on the applicant. We could also simplify what is required when applying to renew an exemption.
- while decisions to grant or decline an exemption are judicially reviewable, small and low-risk businesses are unlikely to use this due to the costs involved. This potentially creates disadvantages for smaller businesses. There is no legislative avenue for businesses to appeal a decision and ask the Ministry to reconsider an application, although in practice businesses are provided with an indication of the Ministry’s intended recommendation and provided with an opportunity to provide comment.



- 1.14. Are exemptions still required for the regime to operate effectively? If not, how can we ensure AML/CFT obligations are appropriate for low-risk businesses or activities?
- 1.15. Is the Minister of Justice the appropriate decision maker for exemptions under [section 157](#), or should it be an operational decision maker such as the Secretary of Justice? Why or why not?
- 1.16. Are the factors set out in [section 157\(3\)](#) appropriate?
- 1.17. Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?
- 1.18. Should the Act specify what applicants for exemptions under [section 157](#) should provide? Should there be a simplified process when applying to renew an existing exemption?
- 1.19. Should there be other avenues beyond judicial review for applicants if the Minister decides not to grant an exemption? If so, what could these avenues look like?
- 1.20. Are there any other improvements that we could make to the exemptions function? For example, should the process be more formalised with a linear documentary application process?

Mitigating unintended consequences

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.

De-risking

One area where our AML/CFT regime has had unintended consequences is that it has made it hard for certain types of businesses, particularly money remittance businesses, to open or maintain a bank account. Known as ‘de-banking’ or ‘de-risking’, these businesses are affected because banks would rather *avoid* rather than *manage* the risk of having the business as a customer. This lack of appetite could be for a variety of reasons: it could be due to concerns from correspondent banking relationships, it could be a desire to avoid reputational damage, or it could be because the cost of managing the risk outweighs the potential profits from having that business as a customer.

However, de-risking has resulted in fewer remittance services operating legitimately and has increased the costs of using those businesses. This ultimately hurts communities in New Zealand and overseas, particularly where there is a cultural expectation of sending money to support families in other countries. A large number of overseas communities rely on remittances: for example, India was the top recipient of remittances in 2020, and the World Bank reports that 40%

of Tonga's GDP comes from remittances. It is important that people can continue to remit funds through safe and legitimate businesses and without paying large fees. However, we also need to balance this against the prerogative of businesses to make commercial decisions about how they operate and who they transact with.⁵

Financial inclusion or exclusion

Financial inclusion or exclusion refers to how well various groups of society, including low income, rural and undocumented persons can access or be provided with adequate range of safe, convenient and affordable financial services (e.g. bank accounts). We recognise that the regime has negatively impacted financial inclusion for some people, either because they are viewed as being risky or because they lack the necessary documentation to prove their identity or address. This is particularly an issue for people without secure access to housing.

Financial inclusion is important because it allows people to more easily participate within society, helps reduce inequality, empowers communities and drives economic growth. Many employers will only pay income into a bank account and it can also be difficult to access benefits or government support without one. As such, we are interested in understanding what barriers there are to financial inclusion and how we can resolve or reduce those barriers.



- 1.21. Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?
- 1.22. How could the regime better protect the need for people to access banking services to properly participate in society?
- 1.23. Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them?

The role of the private sector

Partnering in the fight against financial crime

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

⁵ *E-Trans International Finance Limited v Kiwibank Limited* [2016] NZHC 1031

Zealand Police, New Zealand Customs Service, and several banks, which was established to enable better collaboration on investigating financial crimes.



- 1.24. Can the Act do more to enable private sector collaboration and coordination, and if so, what?
- 1.25. 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?
- 1.26. Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime?

Helping to ensure the system works effectively

Section 3(2) states that the Act facilitates cooperation amongst reporting entities, AML/CFT supervisors, and other government agencies. However, there is no mechanism in the Act that provides for a cooperation or feedback mechanism between the private sector and government, and the private sector is unable to participate in the AML/CFT National Coordination Committee.⁶

Some AML/CFT agencies run their own forums and groups for public/private engagement and partnership and regularly conduct informal engagement with the private sector. For example, DIA maintains an “Industry Advisory Group” that meets approximately four times a year. This group aims to create an effective two-way channel for private/public partners to raise issues, provide feedback and work together to create solutions. RBNZ likewise regularly engage with the New Zealand Banker’s Association, and all supervisors regularly attend AML/CFT conferences together with a large number of private sector attendees.

However, there is no specific forum that is set up to enable private sector discussion and feedback about the operation and performance of the Act on an ongoing basis. We want to explore whether the Act should include a mechanism that better enables this feedback to be provided, and if so, what that mechanism could look like.



- 1.27. Should the Act require have 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?

Powers and functions of AML/CFT agencies

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.

⁶ Section 150(2) requires that any person invited to join the AML/CFT Coordination Committee must be employed in a government agency.

- **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.



- 1.28. 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?
- 1.29. 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?

Providing for ongoing monitoring of transactions and accounts

Under [section 143](#), the FIU is currently able to request that businesses produce or provide access to any information that is relevant to analysing financial intelligence that has been received (e.g. a SAR). However, the FIU is unable to require businesses to provide this information on an ongoing basis, particularly in respect highly risky individuals. The current power therefore carries a risk that information may not be provided in a timely manner and before funds move offshore. In addition, this power can only be used once financial intelligence has been received under the Act and cannot be used in respect of information obtained through other means.

We want to explore whether the power in section 143 should be expanded to allow the FIU to conduct ongoing monitoring of accounts. This would enable the FIU to receive real-time information about the activity that highly risky individuals are engaging in, which could be relevant to potential criminal or civil investigations. Any such power would need to be tightly constrained (e.g. imposing strict time limits, limitations on when the power can be used, and/or requiring judicial authorisation) to ensure there are adequate privacy and human rights safeguards.



- 1.30. Should the FIU be able to request information from businesses on an ongoing basis? Why or why not?
- 1.31. If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?

Freezing or stopping transactions to prevent harm

We would like to explore whether the FIU (or the Commissioner of Police) should have power to freeze assets and stop transactions. This power could enable future harm to be prevented, particularly in instances of child sexual exploitation, human trafficking, scams, frauds, and terrorism financing. Some financial crimes, such as romance or investment scams, can result in repeated victimisation over months or years. A freezing power could help stop a pattern of victimisation at a much earlier point and thereby reduce harm.

If we developed a freezing power, we would need to:

- develop the scope and nature of the power in consultation with the private sector;
- ensure the power is in proportion to the harm being avoided (e.g., making it a short-term freeze, such as for 72 hours).
- ensure that the power does not undermine the willingness of businesses to make reports and that there is a close working relationship and cooperation between businesses and the FIU; and
- ensure that any freezing action does not inadvertently tip off any suspected criminals.



- 1.32. 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?
- 1.33. How can we avoid potentially tipping off suspected criminals when the power is used?

Supervising implementation of targeted financial sanctions

No agency has the authority to supervise or enforce whether businesses are complying with these obligations. This was identified as a significant gap in our Mutual Evaluation which undermines our effectiveness in imposing targeted financial sanctions (see paragraphs 287-288).

Chapter 6, Recommended Action (e) for Immediate Outcome 3 (page 118)

An appropriate agency or agencies should be given clear powers and mandate to supervise and enforce TFS obligations, including establishing clear supervisory expectations for preventive measures to avoid TFS contraventions (e.g., timing and frequency of customer

and transaction screening) and conducting outreach to reporting entities about these expectations (see IO.10).

We would like to understand which agency or agencies should be empowered to monitor and enforce compliance with TFS obligations. It could be the AML/CFT supervisors, given they have relationships with businesses and are already supervising them for compliance with AML/CFT obligations. However, it could be another agency entirely given TFS obligations are not exactly the same as AML/CFT obligations.



- 1.34. Should supervision of implementation of TFS fall within the scope of the AML/CFT regime? Why or why not?
- 1.35. Which agency or agencies should be empowered to supervise, monitor, and enforce compliance with obligations to implement TFS? Why?

Secondary legislation making powers

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.



- 1.36. 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?
- 1.37. How could we better use secondary legislation making powers to ensure the regime is agile and responsive?

Codes of Practice

Codes of Practice can be issued by a Minister responsible for an AML/CFT supervisor (i.e. the Minister of Finance, Minister of Internal Affairs, or the Minister of Commerce and Consumer Affairs). Codes of Practice are intended to set out how businesses can comply with specific obligations and provide a legislative “safe harbour.”

However, in practice, the process for issuing Codes of Practice is burdensome and only one Code has been issued related to identity verification. This means that the value of Codes of Practice has not yet been realised to provide more prescriptive guidance to businesses, and we have instead relied on issuing non-binding guidance. In addition, the Police is responsible for reporting under Act, but does not have a corresponding ability to issue a Code of Practice.

Businesses can “opt out” of a Code if they comply with their obligation by “some other equally effective means” ([section 67\(1\)\(b\)](#)). This is designed to allow businesses flexibility with how they comply, however, by requiring the other means to be “equally effective”, it could mean that there are limited alternative options for businesses other than the Code.



- 1.38. 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?
- 1.39. 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?
- 1.40. 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?
- 1.41. 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?
- 1.42. What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool?

Forms and annual report making powers

The format of annual reports, formal warnings, and various reports (e.g. suspicious activity reports) are prescribed in regulation. Prescribing forms in regulations limits the ability for agencies to quickly change the format of any reports as necessary as all changes need to go through Cabinet and be provided to the Governor-General.

We want to explore whether operational decision makers should be able to make or amend the format of forms and/or reports under the Act. For example, the Act could empower the Commissioner of Police to make or amend the suspicious activity report format, or the chief executives of the supervisors to make or edit the format of annual reports. This would enable agencies to be more responsive to industry needs.



- 1.43. 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?
- 1.44. 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?

AML/CFT Rules

One type of secondary legislation that other countries have made use is AML/CFT Rules. For example, [Australia has issued Rules](#) which are binding on businesses and provide more prescriptive obligations. Other regulatory regimes in New Zealand allow for Rules to be issued, for example the *Land Transport Act 1998*. AML/CFT Rules could allow greater detail and prescription to be provided where appropriate and could be used to provide further clarity about obligations. Rules would have the benefit of being enforceable (unlike guidance) but may not be

able to be opted out of (unlike Codes of Practice). If we allowed for AML/CFT Rules to be issued, we would need to carefully consider who is responsible for issuing them to ensure rules are efficient and effective.



- 1.45. Would AML/CFT Rules (or similar) that prescribed how businesses should comply with obligations be a useful tool for business? Why or why not?
- 1.46. If we allowed for AML/CFT Rules to be issued, what would they be used for, and who should be responsible for issuing them?

Information sharing

Direct data access to FIU information for other agencies

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.

- 1.47. 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?
- 1.48. Are there any other privacy concerns that you think should be mitigated?
- 1.49. 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**?



Data matching to combat other offending

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.



- 1.50. 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?
- 1.51. 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?

Licensing and registration

Registration for all reporting entities

Most, but not all, businesses that have AML/CFT obligations have some other form of requirement to be registered and/or licensed⁷ that is not imposed by the AML/CFT Act. However, there are number of large gaps in terms of which businesses are required to register, meaning that supervisors, particularly the DIA, are unable to easily identify which businesses they supervise.

We want to explore whether we should develop a registration regime that is specific to the AML/CFT regime. An AML/CFT registration regime would enable supervisors to clearly identify which businesses they are required to supervise. It could also enable greater certainty about which sector a business falls into depending on the activities or services they provide. However, we would have to consider how any AML/CFT registration framework interacts with existing registration requirements, e.g. registration on the Financial Services Providers Register.

⁷ **Licensed** means that the business needs to satisfy objective criteria to demonstrate that they are suitable to provide the business activity and requires agencies to actively approve the business to carry out the relevant activity. It can also allow the licensing agency to impose limits or conditions on how the business operates. **Registered**, by contrast, usually does not require the business to satisfy the various criteria, except that they intend to provide the relevant activity and potentially satisfy a fit-and-proper test.

Chapter 6, Recommended Action (a) for Immediate Outcome 3 (page 118)

New Zealand should address the shortcomings relating to licensing and registration of [financial institutions] and DNFBPs. New Zealand should consider setting up a registration regime specific to the AML/CFT Act to ensure the completeness of reporting entities being supervised.

In addition, some high-risk businesses – particularly money remitters, virtual asset service providers, and trust and company service providers⁸ – are only subject to limited fit-and-proper checks before being able to offer the services. This means that there is a greater risk of these businesses being owned or controlled by criminals or their associates. If we developed an AML/CFT registration regime, we could include sufficient fit-and-proper checks as part of the registration process. This would help ensure criminals or their associates are unable to hold (or be the beneficial owner of) a significant or controlling interest in a business or holding a management function.



- 1.52. Should there be an AML/CFT-specific registration regime which complies with international requirements? If so, how could it operate, and which agency or agencies would be responsible for its operation?
- 1.53. If such a regime was established, what is the best way for it to navigate existing registration and licensing requirements?
- 1.54. Are there alternative options for how we can ensure proper visibility of which businesses require supervision and that all businesses are subject to appropriate fit-and-proper checks?

AML/CFT licensing for some reporting entities

We also want to explore including a licensing framework in the AML/CFT regime. A licensing framework would involve agencies (e.g. AML/CFT supervisors) making a positive assessment about whether a business should provide particular services. The licensing authority/ies could also impose conditions through a license which manages or restricts activities in certain circumstances, or more generally impact how the business operates.

A licensing regime would likely be risk based, and only be used for businesses which are at high risk of being misused for money laundering and terrorism financing and are not currently required to be licensed. For example, the Act could require remitters, trust and company service providers, and virtual asset service providers to hold licenses instead of only being registered. If we did this, agencies could further mitigate the risks for those businesses and the sector overall. A licensing regime could also provide greater assurance to those businesses where they are a customer: for example, a bank may have greater assurance about having a remittance business as a customer if they are licensed.

However, while an AML/CFT license regime could be useful for these purposes, licensing frameworks tend to be expensive and administratively burdensome for both the applicant and the

⁸ Only trust and company service providers who are not lawyers or chartered accountants are not subject to any fit-and-proper tests, and the fit-and-proper checks required by the FSPR only applies the person who owns more than 50% of the financial service provider and do not cover beneficial owners or associates.

licensing authority/ies. If we developed an AML/CFT licensing regime we would need to ensure the process does not impose disproportionate compliance costs.



- 1.55. Should there also be an AML/CFT licensing regime in addition to a registration regime? Why or why not?
- 1.56. If we established an AML/CFT licensing regime, how should it operate? How could we ensure the costs involved are not disproportionate?
- 1.57. Should a regime only apply to sectors which have been identified as being highly vulnerable to money laundering and terrorism financing, but are not already required to be licensed?
- 1.58. If such a regime was established, what is the best way for it to navigate existing licensing requirements?
- 1.59. Would requiring risky businesses to be licensed impact the willingness of other businesses to have them as customers? Can you think of any potential negative flow-on effects?

Registration or licensing fee

A prospective AML/CFT-specific registration or licensing regime would require some form of cost recovery or levy to be imposed to pay for the ongoing operational costs, particularly where businesses need to be licensed. This could be in the form of a fee that businesses pay when they apply or renew their registration or license, and this approach would be consistent to how other existing licensing and registration regimes operate.

The levy could also be used more generally to pay for some or all of the operating costs of the AML/CFT regime. This could make the regime more responsive, for example by enabling agencies to provide more detailed guidance, enact faster regulatory changes to resolve compliance challenges, and conduct more in-depth supervision. It could also enable the establishment of a dedicated AML/CFT workforce that is shared between the relevant agencies and allow for people to gain experience in a variety of sectors and roles.

Chapter 6, Recommended Action (c) for Immediate Outcome 3 (page 118)

New Zealand should ensure the appropriate scope and depth of supervision for all the different categories of its supervisory population taking into account the sector-specific vulnerabilities, particularly the higher risks of the banking sector, and provide appropriate levels of resourcing to RBNZ.

Some countries operate a direct cost-recovery model for the AML/CFT regime. For example, Australia charges an Industry Contribution Levy, which entirely pays for the operating costs of AUSTRAC, the Australian FIU and AML/CTF supervisor. However, we also recognise that the compliance costs of AML/CFT can be significant, particularly for smaller businesses. Creating an additional cost to business in the form of a levy would likely add to business costs, particularly in the short term.



- 1.60. Would you support a levy being introduced for the AML/CFT regime to pay for the operating costs of an AML/CFT registration and/or licensing regime? Why or why not?
- 1.61. If we developed a levy, who do you think should pay the levy (some or all reporting entities)?
- 1.62. Should all reporting entities pay the same amount, or should the amount be calculated based on, for example, the size of the business, their risk profile, how many reports they make, or some other factor?
- 1.63. Should the levy also cover some or all of the operating costs of the AML/CFT regime more broadly, and thereby enable the regime to be more flexible and responsive?
- 1.64. If the levy paid for some or all of the operating costs, how would you want to see the regime's operation improved?

Scope of the AML/CFT Act

This review provides an opportunity to identify and examine any potential gaps in the operation of the regime. It is important to consider whether we are capturing all the right activities and businesses to mitigate our national risks of money laundering and terrorism financing. It is also important to ensure the existing ways we capture activities are fit-for-purpose, especially given technological advancements.

Guiding questions for this section:

- Is the scope of currently captured sectors correct? Are there other sectors that should have AML/CFT obligations because of their risks, or excluded because they have low risks?
- Do we need to modernise or update any definitions of captured activities, especially given existing and potential future developments in technology?
- Is it clear which agency is responsible for each sector?

Challenges with existing terminology

“In the ordinary course of business”

Activities only attract obligations if they are provided in the “ordinary course of business”. This is included to ensure that businesses which provide financial services as their business have AML/CFT obligations, but not capture one-off or infrequent activities or transactions.

The AML/CFT supervisors have issued guidance for reporting entities to determine whether an activity is in the ordinary course of business, but there is no legal test in the Act for when something is, or is not, in the ordinary course of business. We also note that there is case law on the interpretation of ‘ordinary course of business’ in the context of other legislation, such as the Companies Act 1993.

For DNFBPs, there are challenges when determining whether an activity is provided in the ordinary course of business. Some non-financial activities may, by definition, only be provided by a DNFBP infrequently, and alongside a much wider array of non-captured services. This leads to considerable confusion about the point at which a captured activity is undertaken in the ordinary course of business, such that the business becomes a reporting entity under the Act. In addition, the FATF recommends DNFBPs comply with AML/CFT obligations, irrespective of whether or not the DNFBP activity is provided in the ordinary course of business.

One solution could be to remove the word “ordinary” from the definition of “designated non-financial businesses and profession”. This would provide certainty and mean the activity is captured and would attract obligations if it is ever conducted, irrespective of how frequently this occurs. These sectors would then have assurance as to whether they have obligations and decide whether or not to continue to provide the activity.

However, removing “ordinary” would also mean that businesses would have to develop full compliance programmes for potentially one-off activities which would result in significant and

potentially disproportionate compliance costs. If we removed “ordinary” for DNFBP activities, we would need to carefully consider how to provide some relief (e.g. an exemption from the requirement to establish a compliance programme) for businesses which only provide one-off activities.



- 2.1. How should the Act determine whether an activity is captured, particularly for DNFBPs? Does the Act need to prescribe how businesses should determine when something is in the “ordinary course of business”?
- 2.2. If “ordinary course of business” was amended to provide greater clarity, particularly for DNFBPs, how should it be articulated?
- 2.3. Should “ordinary” be removed, and if so, how could we provide some regulatory relief for businesses which provide activities infrequently? Are there unintended consequences that may result?

Businesses providing multiple types of activities

Some businesses provide activities which fall within multiple ‘categories’ within the Act, e.g., a bank (financial institution) which sets up companies (a DNFBP activity). However, [section 6\(4\)](#) sets out that the Act applies to a reporting entity *only to the extent* that a financial institution carries out financial institution activities or DNFBPs carry out DNFBP activities.

The policy intent is that a business should be required to apply AML/CFT obligations to mitigate the risks associated with all the activities it offers that are captured under the Act, irrespective of the ‘type’ of reporting entity the business is. We could remove the words “only to the extent” from [section 6\(4\)](#), to ensure the risks of activities are mitigated irrespective of the type of business providing the activity. This change would also avoid any competitive advantage businesses may have and ensure all businesses that provide the particular activity have the same obligations.



- 2.4. Should businesses be required to apply AML/CFT measures in respect of captured activities, irrespective of whether the business is a financial institution or a DNFBP? Why or why not?
- 2.5. If so, should we remove “only to the extent” from [section 6\(4\)](#)? Would anything else need to change, e.g. to ensure the application of the Act is not inadvertently expanded?

In the interim, we could issue regulations that clarify that captured activities attract AML/CFT obligations irrespective of the type of reporting entity which provides those activities. For example, regulations could declare that a financial institution that also provides activities listed under the DNFBP definition must comply with the Act in relation to the DNFBP activities. However, this would also mean that hybrid businesses would be required to file two annual reports (one for the financial institution activities and another for the DNFBP activities). We could exempt hybrid businesses from one or the other obligations to avoid unnecessary duplication.

- 2.6. Should we issue regulations to clarify that captured activities attract AML/CFT obligations irrespective of the type of reporting entity which provides those activities? Why or why not?



“Managing client funds”

Overlap between “managing client funds” and financial institution activities

The DNFBP activity of “managing client funds” (other than sums paid as fees for professional services), accounts, securities, or other assets” overlaps with some financial institution activities such as “transferring money or value for, or on behalf of, a customer” (para (a)(iv)) and “investing, administering, or managing funds or money on behalf of other persons” (para (a)(xi)).⁹ All these activities envisage the active handling of a customer’s money or assets, which include making any transactions on their behalf.

Due to the definition of “trust and company service provider” which includes all other businesses which manage client funds, many businesses could be captured as both a financial institution and DNFBP in relation to the same activity. It is not clear what distinction, if any, there is or should be between “managing client funds” and the other financial institution activities. It is also not clear whether businesses other than ‘true’ DNFBPs should be captured for managing client funds.



- 2.7. Should we remove the overlap between “managing client funds” and other financial institution activities? If so, how could we best do this to avoid any obligations being duplicated for the same activity?

“Sums paid as fees for professional services”

The definition of managing client funds states “(other than sums paid as fees for professional services)”. DIA has taken the view that ‘professional fees’ means a business’ own fees (rather than a third party’s fees), but this position is not clearly stated in the Act. We could clarify what is meant by ‘professional fees’ to provide greater certainty to DNFBPs, and it is unlikely to have a significant impact on New Zealand’s risks.



- 2.8. Should we clarify what is meant by ‘professional fees’? If so, what would be an appropriate definition?
- 2.9. Should the fees of a third party be included within the scope of ‘professional fees’? Why or why not?

⁹ “Managing client funds” also overlaps with “managing individual or collective portfolios” (para (a)(ix)) and “safe keeping or administering of cash or liquid securities on behalf of other persons” (para (a)(x));

“Engaging in or giving instructions”

Businesses which engage in or give instructions on behalf of a customer for certain activities are intended to have AML/CFT obligations. This is intended to capture those businesses which are involved in preparing and assisting customers to undertake various specified activities where there is a risk of money laundering and terrorism financing, including the operation and management of legal persons and arrangements. However, the meaning of the phrase “engaging in or giving instructions” is not clear and could be clarified. For example, we could change “engaging in” to “assisting a customer to prepare for” the activities listed in paragraphs (vi)(A) to (E).



- 2.10. Does the current definition appropriately capture those businesses which are involved with a particular activity, including the operation and management of legal persons and arrangements? Why or why not? How could it be improved?
- 2.11. Have you faced any challenges with interpreting the activity of “engaging in or giving instructions”? What are those challenges and how could we address them?

Definition of financial institution activities

The terminology used in the definition of financial institution was drawn from the FATF’s definition. However, the terminology does not correlate with the terms used in the definition of financial service provider in [section 5](#) of the *Financial Service Providers (Registration and Dispute Resolution) Act 2008* (FSP Act). For example, being a registered bank is captured as a financial service in the FSP Act, but there is no equivalent activity in the AML/CFT Act for banks. Similarly, operating a money or value transfer service is captured as a financial service in the FSP Act, but the Act captures businesses which “transfer money or value for, or on behalf of, a customer”.

The slight differences in approach between the definitions of “financial activity” versus “financial institution” has the potential to cause confusion and inconsistencies for businesses when trying to understand how the Act applies to their business and the risk they are exposed to and who their supervisors are. We could provide further clarity by better aligning the terminology between the FSP Act and AML/CFT Act.



- 2.12. Should the terminology in the definition of financial institution be better aligned with the meaning of financial service provided in [section 5](#) of the *Financial Service Providers (Registration and Dispute Resolution) Act 2008*? If so, how could we achieve this?
- 2.13. Are there other elements of the definition of financial institution that cause uncertainty and confusion about the Act’s operation?

High Value Dealers

Definition of “high-value dealer”

A person only becomes a “high-value dealer” if, in the ordinary course of business, they buy or sell any high value articles by way of (singular or multiple) cash transactions which equal or exceed NZD 10,000. This means that businesses who never transact in cash (or only do so below the threshold without there being any related cash transactions) are not high-value dealers and can avoid AML/CFT obligations under the Act. However, this also means that businesses who engage in relevant cash transactions occasionally do not meet the definition of a high-value dealer.

The inclusion of “in the ordinary course of business” in the definition of high value dealer is problematic because cash transactions of NZD 10,000 or more may be considered out of the ordinary and occasional. We can provide further clarity for high value dealers, for example by removing “ordinary” from the definition. This would capture all businesses which engaged in cash transactions for high value goods, irrespective of how ‘ordinary’ the transaction is.



- 2.14. Should the definition of high-value dealer be amended so businesses which deal in high value articles are high-value dealers irrespective of how frequently they undertake relevant cash transactions? Why or why not? Can you think of any unintended consequences that might occur?
- 2.15. What do you anticipate would be the compliance impact of this change?

Exemption for pawnbrokers

Pawnbrokers are excluded from the Act, even though they may engage in activities similar to ones that high value dealers engage in. This exclusion was intended to be transitional. Pawnbrokers have obligations under the *Secondhand Dealers and Pawnbrokers Act 2004* which are mostly, but not entirely, in line with the obligations for high value dealers. For example, pawnbrokers have some obligations to conduct CDD and keep records, but these are not consistent with obligations for high value dealers. In addition, pawnbrokers do not have equivalent tipping off protections when reporting stolen goods to the Police.

We want to explore whether we should remove the current exclusion for pawnbrokers and include them within the AML/CFT regime. There are approximately 700 companies with active licenses issued by the Secondhand Dealers and Pawnbrokers Authority. While not all of these businesses would trade high value articles for cash, any pawnbroker which does may not be appropriately mitigating the risks that their business is misused for money laundering and terrorism financing. However, given that there is an existing regime, we need to ensure that we do not duplicate obligations for pawnbrokers and impose unnecessary compliance costs if we removed this exclusion.

- 2.16. Should we revoke the exclusion for pawnbrokers to ensure they can manage their money laundering and terrorism financing risks? Why or why not?
- 2.17. Given there is an existing regime for pawnbrokers, what obligations should we avoid duplicating to avoid unnecessary compliance costs?



Appropriate cash transaction threshold

Buying and selling high value assets is attractive for criminals because these transactions can be less visible to the government and other financial institutions. Many high value assets can be easily hidden and transferred to third parties with limited documentation, and with no transactions visible to other financial institutions.

We recommended that the appropriate threshold for cash transactions should be NZD 10,000 when implementing the amendments to the AML/CFT Act in 2018. We made this recommendation following consultation with industry and considered that a threshold of NZD 10,000 struck the appropriate balance between compliance obligations and providing the FIU with intelligence.

We are concerned that the NZD 10,000 cash threshold for high value dealers and prescribed transactions means that we are missing out on intelligence, particularly where transactions are being structured below NZD 10,000. Lowering the high value dealer threshold (as well as the prescribed transaction threshold, discussed below) would enable better intelligence to be collected and better law enforcement outcomes. A lower threshold could potentially mean that more transactions attract AML/CFT obligations (unless businesses stop transacting in cash).



We also consider the appropriate thresholds for making prescribed transaction reports, including reports of large cash transactions. This is discussed below at page 89.

- 2.18. Should we lower the applicable threshold for high value dealers to enable better intelligence about cash transactions? Why or why not?
- 2.19. If so, what would be the appropriate threshold? How many additional transactions would be captured? Would you stop using or accepting cash for these transactions to avoid AML/CFT obligations?



Stored Value Instruments

Regulation 15 of the AML/CFT (Definitions) Regulations 2011 includes certain types of transactions involving “stored value instruments” as occasional transactions which require CDD. A stored value instrument is defined as a “portable device [...] that is capable of storing monetary value in a form that is not physical currency”. It is intended to capture vouchers and gift cards, as well as travel cards, and the use of ‘portable device’ in the definition implies that the instrument has to be a tangible object. However, other types of stored value instruments have been developed, including those which are not tangible (e.g. purely digital instruments such as email

vouchers). These non-tangible stored value instruments are not currently captured by Regulation 15.

We want to explore whether we should amend the regulation to be neutral as to the form or format of the instrument to capture digital instruments. This would expand the application of this regulation (as well as Regulation 15 of the AML/CFT (Exemptions) Regulations 2011) and mean that more transactions are considered occasional transactions, but it would also mean that the risks of stored value instruments are addressed regardless of the format or technology involved. Australia amended their legislation in 2017 to amend their definition of ‘stored value card’ and inserted a new definition that is explicitly technology neutral.

- 2.20. Do you currently engage in any transactions involving stores of value that are not portable devices (e.g. digital stored value instruments)? What is the nature and value of those transactions?
- 2.21. What risks do you see with stored value instruments that do not use portable devices?
- 2.22. Should we amend the definition of “stored value instruments” to be neutral as to the technology involved? If so, how should we change the definition?



Potential new activities

Acting as a secretary of a company or partner in a partnership

People who act in a position of authority for a legal person can be exposed to money laundering or terrorism financing risks. Currently, the Act captures natural or legal persons who act, or arrange for persons to act, as nominee directors or nominee shareholders or trustees in relation to legal persons or legal arrangements. This does not include persons acting as company secretaries, partners in partnerships, or similar positions in other legal persons. This is not in line with the FATF standards.

A “company secretary” is not a position recognised by the *Companies Act 1993* but is a position recognised in other jurisdictions, such as the United Kingdom. The responsibilities of a company secretary can include acting as a chief administrative officer, controlling the finances of the company, carrying out the instructions of the board, and liaising with shareholders. A secretary or partner has considerable influence over their respective legal person and visibility of the day-to-day operations and acting in those roles on the instruction of a third party can obscure who owns or controls the company or partnership.

We could issue regulations to include businesses and people who act as secretaries for companies, partners in partnerships, or equivalent positions for other legal persons and arrangements in the Act. This would help address money laundering and terrorism financing risks and would bring New Zealand more in line with FATF standards, but it would also impose additional compliance costs on businesses which provide these activities. We do not know how many businesses offer these services (who are not already captured for providing nominee director or shareholder services), but we estimate the number to be low.

- 2.23. Should acting as a secretary of a company, partner in a partnership, or equivalent position in other legal persons and arrangements attract AML/CFT obligations?
- 2.24. If you are a business which provides this type of activity, what do you estimate the potential compliance costs would be for your business if it attracted AML/CFT obligations? How many companies or partnerships do you provide these services for?



Criminal defence lawyers

Lawyers who only provide criminal defence services have no obligations under the Act but may be in a position to identify suspicious activities. For example, they may have a client who insists on paying legal fees in cash, which may indicate that criminal proceeds are being used to pay for their legal defence. We want to explore whether criminal defence lawyers should have some AML/CFT obligations (e.g. to file SARs and report large cash transactions). An obligation to report SARs and large cash transactions would provide the FIU with further intelligence about how criminal proceeds are used.

However, if we imposed obligations on criminal defence lawyers, we would need to carefully navigate questions of whether these obligations are proportionate as well as issues of legal privilege, rights to a fair trial, and lawyers' professional obligations under the *Rules of Conduct and Client Care*.



- 2.25. Should criminal defence lawyers have AML/CFT obligations? If so, what should those obligations be and why?
- 2.26. If you are a criminal defence lawyer, have you noticed any potentially suspicious activities? Without breaching legal privilege, what were those activities and what did you do about them?
- 2.27. Are there any unintended consequences that may arise from requiring criminal defence lawyers to have limited AML/CFT obligations, that we need to be aware of?

Non-life insurance businesses

Only businesses which issue life insurance policies currently have obligations under the Act, as is required by the FATF. However, insurance companies which provide other insurance policies may be in a position to identify suspicious activity or behaviour, such as potential or actual frauds. Insurance policies can also be vulnerable to money laundering, for example where a customer makes an overpayment or requests a refund shortly after purchasing a policy. Insurance fraud can also be used for money laundering, e.g. where a person insures a valuable item which is stolen or destroyed by an accomplice.

Including non-life insurance businesses in the Act could address money laundering vulnerabilities and provide a useful source of financial intelligence. We could also tailor the obligations of non-life insurers to ensure they are in line with the particular risks and vulnerabilities we have

identified by, for example, only requiring non-life insurers to monitor accounts and report suspicious activity.



- 2.28. Should non-life insurance companies become reporting entities under the Act?
- 2.29. If so, should non-life insurance companies have full obligations, or should they be tailored to the specific risks we have identified?
- 2.30. If you are a non-life insurance business, what do you estimate would be the costs of having AML/CFT obligations (including limited obligations)?

Including all types of Virtual Asset Service Providers

Recent years have seen an increase in new and innovative technologies that can be used to swiftly transfer value around the world. Blockchain and distributed ledger technologies have the potential to radically change the financial landscape. Their perceived anonymity, speed and global reach also attracts those who want to escape authorities' scrutiny. Businesses which provide services in respect of virtual assets (e.g. Bitcoin, Ethereum) have been identified internationally as being vulnerable to significant money laundering and terrorism financing risks.

To combat this growing concern, the FATF issued binding standards in 2019 to require countries to take action to understand, identify, and address the risks that virtual asset service providers pose in their country. This includes applying AML/CFT obligations to businesses which provide one of the five types of virtual asset activities identified by the FATF:

1. exchanging between virtual assets and fiat currencies (e.g. New Zealand Dollars);
2. exchanging between one or more forms of virtual assets;
3. transferring (i.e. conducting a transaction on behalf of a person that moves a virtual asset from one virtual asset address or account to another) virtual assets;
4. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
5. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Our existing definition of financial institution is sufficiently broad to capture the first, second, third, and fifth virtual asset activity. However, to ensure all virtual asset service providers are clearly captured, we need to extend obligations to wallet providers which only provide safekeeping or administration of virtual assets. This will ensure that New Zealand is not out-of-step with the rest of the world. We do not anticipate that there would be significant compliance costs as a result of this change. There are a small number of virtual asset service providers operating in New Zealand, and we are not aware of any business which only offers safekeeping or administration of virtual assets.



We also need to consider what obligations virtual asset service providers should have which are in line with the risks they are exposed to. This is discussed in more detail below (see page 88)

2.31. Should we use regulations to ensure that all types of virtual asset service providers have AML/CFT obligations, including by declaring wallet providers which only provide safekeeping or administration are reporting entities? If so, how should we?

2.32. Would issuing regulations for this purpose change the scope of capture for virtual asset service providers which are currently captured by the AML/CFT regime?



Combatting trade-based money laundering

Businesses involved in preparing, processing, and paying invoices and annual reports may detect suspicious activities that could indicate trade-based money laundering, which is a significant global threat. For example, this activity may identify:

- **Over-invoicing**, where an exporter submits an inflated invoice to the importer which generates a payment that exceeds the value of the shipped goods;
- **Under-invoicing**, where an exporter submits a deflated invoice to the importer, shipping goods with greater value and transferring that value to the importer;
- **Multiple invoicing**, where the exporter submits multiple times for the same shipment;
- **Over-invoicing or under-invoicing**, where the exporter ships more (or less) goods to the importer than agreed and invoiced; and,
- **Misrepresentation of quality**, where goods shipped to the importer are misrepresented on official documentation as being of higher or lower quality.
- **Channelling payments through third party jurisdictions**, where exporters receive payments for goods from a different country than the one to which they are exporting.

Following the amendments to the AML/CFT Act in 2017, accountants, tax agents and bookkeepers must carry out AML/CFT obligations for services they provide that attract money laundering and terrorism financing. These types of businesses provide services related to preparing, processing, and paying invoices and therefore may be in a position to detect trade-based money laundering.

Preparing or processing invoices

Accountants, tax agents or bookkeepers (accounting practices) involved in the preparing and processing of invoices may have AML/CFT obligations for that activity. If the accounting practice is also involved in the payment of funds on behalf of the client, then the activity of preparing and processing invoices is part of managing client funds. In addition, preparing and processing invoices may also be 'engaging in or giving instructions for transactions relating to creating, managing or operating a legal person or legal arrangement irrespective of whether the accounting practice is managing the funds of the client.

Capturing this activity in this way may cause confusion and not adequately cover all situations where trade-based money laundering could occur. We could clarify this activity in the Act. This change could also allow us to also adjust obligations for businesses which engage in this activity to ensure compliance costs are in proportion to risks.



- 2.33. Is the Act sufficiently clear that preparing or processing invoices can be captured in certain circumstances?
- 2.34. If we clarified the activity, should we also clarify what obligations businesses should have? If so, what obligations would be appropriate?

Preparing annual accounts and tax statements

Trade based money laundering, fraud, tax evasion, and other criminal activity could also be detected by businesses involved in preparing annual accounts or tax statements for customers. Trade based money laundering does not currently attract AML/CFT obligations unless the business is also involved in managing client funds or engages in or give instructions in relation to transactions.

We could capture the activity of preparing annual accounts and tax statements. This would potentially enable greater detection of trade-based money laundering and other criminality, but it would likely increase the number of businesses that have obligations and the compliance costs for those businesses. In 2017, Inland Revenue estimated that there were approximately 5,600 active tax agents, but it is not known how many of these businesses already have AML/CFT obligations and would therefore become reporting entities as a result of capturing this activity. Irrespective, we could tailor obligations for these businesses if we included this activity, e.g. by only requiring these businesses to report suspicious activities.



- 2.35. Should preparing accounts and tax statements attract AML/CFT obligations? Why or why not?
- 2.36. If so, what would be the appropriate obligations for businesses which provide these services?

Non-profit organisations vulnerable to terrorism financing

Charities and other non-profit organisations have been identified by the FATF as being vulnerable to being misused or exploited for terrorism financing. In New Zealand, registered charities that operate overseas and in high-risk jurisdictions, tax-exempt non-profits that are not registered charities, and non-resident tax charities are the types of non-profit organisations that have some vulnerabilities.¹⁰ However, non-profit organisations that are not registered charities are not subject to monitoring or supervision to ensure they cannot be misused for terrorism financing.¹¹ This is a gap in New Zealand's regime that could be exploited.

Chapter 4, Recommended Action (e) for Immediate Outcome 10 (page 84)

New Zealand should consider options to increase monitoring or supervision of those charities identified as having a moderate vulnerability to abuse for terrorism financing under the NRA.

¹⁰ *National Risk Assessment 2019*, page 24. Available at: <https://www.police.govt.nz/sites/default/files/publications/fiu-nra-2019.pdf>

¹¹ Charities regulated by Charities Services and the Charities Registration Board have some obligations that mitigate terrorism financing risks.

We want to explore whether the Act could be used to mitigate the vulnerabilities of non-profit organisations at risk of being misused for terrorism financing which are not registered charities. One option for mitigating the vulnerabilities that we have identified would be to include tax-exempt non-profits and non-resident tax charities within the AML/CFT regime and treat them as a type of reporting entity with obligations that are targeted towards addressing the particular terrorism financing risks to which they are exposed. These obligations could include:

- requiring organisations to maintain information on the purpose of their activities, the identity of the person(s) who own the organisation, control, or direct their activities, including senior officers, board members, and trustees.
- providing financial statements that provide detailed breakdowns of income and expenditure.
- requiring appropriate controls or compliance programmes to ensure that all funds are fully accounted for and spent in an appropriate manner.
- an obligation to take reasonable measures to confirm the identity, credentials and good standing of persons or groups who benefit from the organisations works, as well as associate organisations.

However, including tax-exempt non-profits and non-resident tax charities in the AML/CFT regime would have potentially significant compliance costs for these organisations. We would need to ensure that any measures are risk-based and in proportion to the organisation's vulnerability to being misused for terrorism financing and did not undermine the ability of these organisations to provide charitable services.



2.37. Should tax-exempt non-profits and non-resident tax charities be included within the scope of the AML/CFT Act given their vulnerabilities to being misused for terrorism financing?

2.38. If these non-profit organisations were included, what should their obligations be?

Currently exempt sectors or activities

As discussed above at page 5, the FATF considered that New Zealand had granted a large number of exemptions, and not all of these were granted in cases of proven low money laundering and terrorism financing risks. This review provides an opportunity to consider existing regulatory exemptions and class exemptions to ensure they reflect situations of proven low risk.

2.39. Are there any other regulatory or class exemptions that need to be revisited, e.g. because they no longer reflect situations of proven low risk or because there are issues with their operation?



Internet auctioneers and online marketplaces

The Act excludes all services provided by internet auction providers.¹² The definition of ‘internet auction provider’ is broad and applies to all processes “operated online to enable members of the public to conclude contracts for the sale and purchase of goods or the provision and acquisition of non-financial services”. The scope of the exclusion is also broad and applies to all captured activities that the internet auction provider offers, regardless of the risks associated with that activity in an internet auction setting.

The number of online marketplaces which enable third party vendors to list products for sale has increased in recent years. These online marketplaces fall within the scope of this exemption, even though they do not strictly provide an internet auction service. The scope of the exclusion is broad and applies to all captured activities that the internet auction provider offers, regardless of the risks associated with that activity in an internet auction setting. We have identified some risks regarding online marketplaces as they could be used to facilitate a domestic form of trade-based money laundering, and therefore want to ensure whether this exemption is still appropriate or whether it needs to be changed in some way.

- 2.40. Should the exemption for internet auctions still apply, and are the settings correct in terms of a wholesale exclusion of all activities?
- 2.41. If it should continue to apply, should online marketplaces be within scope of the exemption?
- 2.42. What risks do you see involving internet marketplaces or internet auctions?
- 2.43. If we were to no longer exclude online marketplaces or internet auction providers from the Act, what should the scope of their obligations be? What would be the cost and impact of that change?



Special remittance card facilities

Businesses which offer certain types of remittance card facilities have a limited exemption from customer due diligence obligations.¹³ This exemption was aimed at facilitating cross-border remittances to the Pacific given the difficulties that remittance providers have faced in accessing the formal financial system. However, we want to ensure that this exemption reflects our money laundering and terrorism financing risks and would like to understand how many businesses currently rely on this exemption, how it operates, and whether it appropriately manages risks involved with remittance cards.

- 2.44. Do you currently rely on this regulatory exemption to offer special remittance card facilities? If so, how many facilities do you offer to how many customers?



¹² AML/CFT (Definitions) Regulations 2011, [regulation 21A](#)

¹³ AML/CFT (Exemptions) Regulations 2011, [regulation 10](#)

- 2.45. Is the exemption workable or are changes needed to improve its operation? What would be the impact on compliance costs from those changes?
- 2.46. Do you consider the exemption properly mitigates any risks of money laundering or terrorism financing through its conditions?

Non-finance businesses which transfer money or value

Regulation 18A AML/CFT (Definitions) Regulations 2011 exempts non-finance businesses involved in transferring money to facilitate purchase of goods or services. The exemption was originally intended to exempt non-finance businesses, primarily retail organisations (e.g., travel agents), that provide captured financial activities from being financial institutions. A "non-finance business" is defined in Reg 18A(2) as "a person whose only or principal business is the provision of goods or services that are not relevant services".

This regulation has become problematic after the Act was amended in 2017 to include DNFBPs. This is because DNFBPs are, by definition, "non-finance businesses", and some DNFBPs regularly transfer money to facilitate the purchase and goods or services that are not relevant services. When this constitutes 'managing client funds' it is intended to attract AML/CFT obligations. However, this is currently unclear and could be clarified.

- 2.47. Should we amend this regulatory exemption to clarify whether and how it applies to DNFBPs? If so, how?



Potential new regulatory exemptions

This review provides an opportunity to make new regulatory exemptions for categories of businesses or transactions which are demonstrably low risk. This includes consolidating existing Ministerial exemptions into regulatory exemptions which makes the exemptions more permanent as they do not expire.

- 2.48. Should we issue any new regulatory exemptions? Are there any areas where Ministerial exemptions have been granted where a regulatory exemption should be issued instead?



Acting as a trustee or nominee

Acting as a trustee or nominee director or shareholder attracts AML/CFT obligations. DNFBPs that provide this service for clients often do so by using or creating a separate company to act as the actual trustee or the nominee shareholder. Typically, the company is a wholly owned subsidiary of the DNFBP which has been engaged to provide the trustee or nominee service. However, the trustee or nominee company have AML/CFT obligations in their own right, as they are providing a captured activity in the ordinary course of business.

Persons that act as a trustee or nominee are exposed to significant money laundering risks and should be subject to AML/CFT obligations. However, we acknowledge that there can be significant compliance overlap and burden if each separate trustee or nominee company also individually has AML/CFT obligations. This is particularly so for those DNFBPs that use multiple different legal persons to deliver their trustee or nominee services.

We want to explore whether persons acting as a trustee or nominee should be exempt from being reporting entities or subject to AML/CFT obligations in certain situations. This could include where the nominee or trustee company is a wholly owned subsidiary and a parent DNFBP is responsible for complying with all AML/CFT obligations. We could also include conditions to manage any remaining concerns, such as requiring the parent DNFBP to maintain an up-to-date list of all trustees and nominees it uses to deliver its services, include them in its risk assessment and annual report, and make the list available to its supervisor upon request.

- 2.49. Do you currently use a company to provide trustee or nominee services? If so, why do you use them, and how many do you use? What is the ownership and control structure for those companies?
- 2.50. Should we issue a new regulatory exemption to exempt legal or natural persons that act as trustee, nominee director, or nominee shareholder where there is a parent reporting entity involved that is responsible for discharging their AML/CFT obligations? Why or why not?
- 2.51. If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?



Crown entities, Crown agents etc

Several Crown entities and Crown agents have become captured as reporting entities under the AML/CFT Act. It is important that laws apply equally, however Crown entities generally less exposed to money laundering or terrorism financing as they have additional checks and reporting requirements. For example, Crown entities and agents may be subject to requirements under the *Public Finance Act 1989*, *Crown Entities Act 2004*, and *Public Audit Act 2001*. In addition, Crown entities and agents may be entirely owned by the Crown and only use Crown monies to carry out its activities.

We want to explore whether a regulatory exemption should be issued to exempt wholly owned Crown entities or agents for the Crown (to the extent that this affects a certain part of the business). Several Crown entities and agents have been granted Ministerial exemptions under [section 157](#),¹⁴ so it may be appropriate to exempt these types of entities through regulations given several have already been exempted. This could also include Community Trusts that operate under the *Community Trusts Act 1999*.

¹⁴ [Callaghan Innovation](#), a Crown-owned entity, [Kāinga Ora](#), a Crown agency, and [New Zealand Green Investment Finance Limited](#), a Crown-owned company have all recently received Ministerial exemptions.

- 2.52. Should we issue a new regulatory exemption to exempt Crown entities, entities acting as agents of the Crown, community trusts, and any other similar entities from AML/CFT obligations?
- 2.53. If so, what should be the scope of the exemption and possible conditions to ensure it does not raise other money laundering or terrorism financing vulnerabilities?



Low value loan providers

Generally, providers of low-value loans will be captured as a financial institution as a non-bank non-deposit taking lenders. Although this sector carries some risk (e.g. illicit funds can be able to potentially be used to repay lending) this is significantly reduced in situations where the loans are low value or provided for charitable purposes.

Low-value loans have a role in providing community support and includes social lenders. Social lenders have emerged as a form of financing for parties that may not be eligible for traditional forms of commercial financing. Social lending is not-for-profit and is used to support community projects and social outcomes.

To date, there has been several low value loan exemptions granted and we want to explore whether a regulatory exemption could be more appropriate.¹⁵ These exemptions account for the community function of social lenders and promotion of financial inclusion. The compliance burden is considered disproportionate for low value loan providers, particularly when they are acting not-for-profit as this cost will be passed on to the customer.

- 2.54. Should we issue an exemption for all reporting entities providing low value loans, particularly where those loans are provided for social or charitable purposes?
- 2.55. If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?



Territorial scope

The Act does not set out where business activities need to be conducted in order to attract AML/CFT obligations in New Zealand. For example, there is no test to determine whether an activity provided solely online to New Zealanders by an offshore company attracts obligations, nor whether a New Zealand business which forms or incorporates companies, acts as a trustee or provides financial services wholly offshore should be exempt from obligations under New Zealand law. The absence of any territorial scope provisions in the Act are increasingly raising complex questions of how to determine whether a business or business activity should be subject to AML/CFT obligations in New Zealand.

¹⁵ For example, [Moray Foundation Trust](#), [Just Dollars Trust](#), [Jubilee Christian Charitable Trust](#), [Habitat for Humanity New Zealand Limited and Habitat Affiliates](#), [Wairakei 801 Limited](#), [Newtown Ethical Lending Trust](#).

In an effort to provide certainty to entities and supervisors, guidance has been developed by the three supervisors in consultation with Ministry of Justice, which sets out when a business activity falls within the scope of our AML/CFT regime. However, this guidance may need to be reconsidered, particularly with recent amendments to the *Financial Service Providers (Registration and Dispute Resolution) Act 2008* which now requires providers of financial services to be registered only if they are in the business of providing financial services to persons in New Zealand above a minimum threshold, regardless of where the financial services are provided from.



- 2.56. Should the AML/CFT Act define its territorial scope?
- 2.57. If so, how should the Act define a business or activity to be within the Act's territorial scope?

Supervision, regulation, and enforcement

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?

Agency supervision model

The objectives of supervision are to ensure that businesses understand their obligations, maintain appropriate AML/CFT internal controls, and that non-compliant businesses are subject to effective, proportionate, and dissuasive sanctions.

We considered different supervisory models in the process of developing the Act, including the Australian model of a single supervisor with the Financial Intelligence Unit embedded within it. We also considered various combinations of multiple supervisors, including involving self-regulatory bodies (such as the Law Society) in supervising their professions. Ultimately, we determined that using government agencies with existing regulatory relationships with sectors was the best approach in the New Zealand context.

The current supervision model involves three different agencies as AML/CFT supervisors:

- the Financial Markets Authority (FMA) supervises a range of businesses, including issuers of securities, licensed supervisors, derivatives issuers, managed investment scheme managers, client money or property service providers, equity crowdfunding platforms, peer-to-peer lending providers, discretionary investment management services and certain financial advice providers,

- the Reserve Bank of New Zealand (RBNZ) supervises registered banks, life insurers, and non-bank deposit takers, and
- the Department of Internal Affairs (DIA) supervises casinos, non-deposit taking lenders, money changers, DNFBPs and high value dealers, and other reporting entities/financial institutions that are not covered within the sectors supervised by FMA or RBNZ.

We have an opportunity to take stock of our supervisory arrangements and determine if there is a need for change now that New Zealand has had time to embed this supervisory model. However, we would need to carefully consider any changes as they would be potentially significant, take a large amount of work, and would require some time to implement. In addition, the FATF did not consider there were any issues with having a split supervisory model or whether such a model can be effective but did recognise that there were differences and potential inconsistencies between each supervisor.



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

Mechanisms for ensuring consistency

The regime needs to ensure an appropriate amount of consistency in how supervisors interpret and apply the law. An inconsistent approach can result in some businesses who may operate across the supervisory sectors to “shop around” for approaches that meet their preference, or unfair treatment across sectors.

In practice, the DIA, FMA, and RBNZ work closely with each other to ensure, where possible, that the AML/CFT supervision is consistent, including through issuing joint supervisory positions through triple branded guidance. However, we recognise that there are some areas of inconsistency that have not been resolved, such as who is required to file prescribed transaction reports.

There are currently limited mechanisms in the AML/CFT Act to ensure consistency in terms of interpretation and application of the law between the supervising agencies, beyond the requirements in [section 131\(e\)](#) for supervisors to cooperate to ensure the consistent, effective, and efficient implementation of the Act. While some inconsistencies can be a result of the differences in the nature of the sectors supervised by each agency, we want to explore whether there are other mechanisms that need to be established to ensure consistency where it is needed while also ensuring supervisors can respond to the needs of their individual sectors.



- 3.3. 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?
- 3.4. 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?

Powers and functions

The functions and the powers of the AML/CFT supervisors are set out in the Act, particularly in [sections 131](#) and [132](#). Broadly, the supervisors have the function of monitoring sectoral risks, monitoring compliance of businesses within its sectors, providing guidance, investigating and enforcing the Act, and otherwise cooperating with other AML/CFT agencies. The Act further states that supervisors have all the necessary powers to carry out these functions, including requiring the production or access to information and conducting onsite inspections in accordance with [section 133](#).



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

Inspection powers

Onsite inspections at dwelling houses

[Section 133\(1\)](#) of the Act enables a supervisor to undertake on-site inspections, including the ability to enter and remain at any place for the purpose of conducting an onsite inspection of a reporting entity. The section specifically limits this power by excluding dwelling-houses and marae. DIA and FMA supervise a number of reporting entities, including high-risk entities, who may operate out of the business owner's home.

The exclusion under [section 133\(1\)](#) prevents DIA and FMA from exercising its statutory powers of onsite inspection for these reporting entities. We would like to ensure that the Act is clear that onsite inspections of dwelling houses is possible, but we also want to ensure that the rights of occupants are protected. DIA has previously undertaken inspections "by consent" at a reporting entity that is also a dwelling house. While this has been appropriate thus far, challenges of admissibility of evidence could arise for enforcement action against a business which had been inspected "by consent at a dwelling house".

Remote inspections

The COVID-19 pandemic has meant that businesses and agencies have had to operate differently, including looking for opportunities to work remotely across the AML/CFT system. Supervisors can remotely issue notices for records, documents, or information. However, there are no provisions allowing off-site supervisory engagements to be undertaken (e.g. interviews by video conferencing, phone calls, remote testing) rather than physical onsite inspections. This posed logistical challenges during lockdowns. The same challenges can arise for businesses which conduct their business remotely and without a physical office.

Outside of pandemic situations, undertaking supervisory engagements remotely would be more efficient in situations that do not require a physical on-site inspection. The flexibility of remote supervision may also benefit reporting entities and allow for more responsive supervision. We want to explore whether supervisors should be able to conduct remote inspections, and if so, what a remote inspection would require.



- 3.6. Should AML/CFT Supervisors have the power to conduct onsite inspections of reporting entities operating from a dwelling house? If so, what controls should be implemented to protect the rights of the occupants?
- 3.7. What are some advantages or disadvantages of remote onsite inspections?
- 3.8. Would virtual inspection options make supervision more efficient? What mechanisms would be required to make virtual inspections work?

Approving the formation of a Designated Business Group

Supervisors have the power to approve the formation of a designated business group (DBG), including adding additional members. However, the current process does not include a stage where the supervisor considers whether to approve (or reject) the formation of the DBG, unless the supervisor has requested further information and indicated the entity is ineligible to form or join a DBG. We want to ensure the process is appropriate and are interested to explore whether the process should include an explicit approval step where a supervisor can approve or reject the formation of a DBG.

- 3.9. Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient?
- 3.10. Should supervisors have an explicit role in approving or rejecting the formation of a DBG? Why or why not?



Regulating auditors, consultants, and agents

Independent auditors

There have been ongoing issues and questions from the sector and the AML/CFT agencies about the quality of the audits, who can conduct them, whether there is an expected level of quality (assurance) and even what an audit is. The supervisors published an Audit Guideline in 2012 to try and address some of these issues, which was revised in 2019 where reciprocal auditing was introduced.

However, despite the Guideline, there continue to be wide variations in the quality of independent audits that businesses receive and, in turn, are using to make improvements to approaching their obligations. We want to explore whether the requirements for audits should be prescribed in more detail, including what is meant by “appropriately qualified”. This could improve the quality of audits provided and make the process more useful for businesses and supervisors. We could also set out whether there should be any protection or allowance for businesses which rely on audits, and whether there should be any liability for auditors who do not conduct a satisfactory audit.



We consider the scope of what is required by an audit or review, including what actions could result below at page 91.



- 3.11. 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?
- 3.12. Who would be responsible for enforcing the standards of auditors?
- 3.13. What impact would that have on cost for audits? What benefits would there be for businesses if we ensured higher quality audits?
- 3.14. Should there be any protections for businesses which rely on audits, or liability for auditors who do not provide a satisfactory audit?

Consultants

Since the Act came into force, a number of consultants have been providing services to reporting entities to help them meet their AML/CFT obligations. We did not anticipate the potential role of consultants in supporting businesses with complying with AML/CFT when we were developing the Act.

Generally, consultants are providing advice which helps raise compliance levels across the system. However, there are no standards or registration and licensing requirements for providing consultancy services, which has resulted in a range of quality of advice being provided to businesses. It is also unclear what recourse businesses or regulators have against consultants who give poor or inaccurate advice upon which a business has subsequently relied.

As the AML/CFT system matures supervisors have signalled that they will increase the focus on enforcement. The disparity in advice value will cause increased regulatory risk for entities receiving poor advice. The High Court in the *Department of Internal Affairs v Qian DuoDuo Limited* [2018] NZHC 1887 explicitly considered the role of the consultant and reduced the penalty imposed due to the business relying on advice which did not identify compliance failures. Given this judgment, we want to explore whether the Act should better recognise the role that consultants play and provide for some appropriate regulation.



- 3.15. 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?
- 3.16. 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?
- 3.17. Who would be responsible for enforcing the standard of consultants?

Agents

Some businesses rely on and appoint agents to carry out some or all their obligations. For example, some businesses may rely on agents to conduct CDD or submit SARs. Agents are commonly used by money or value transfer service providers (e.g. remitters) but all types of businesses can use agents and third parties to act on their behalf. There are a number of benefits for doing so – it can improve the application of the legislation and enable obligations to be complied with in a more efficient manner.

However, the Act does not currently set standards for who can be an agent, nor are agents required to be licensed or registered (see page 15). The lack of any standards or registration and licensing requirements for agents risks criminals or their associates from providing services on behalf of a registered or licensed business and exposing that business to money laundering and terrorism financing risks.

In addition, the Act does not specify what agents can be relied on beyond conducting CDD ([section 34](#)). Some businesses, such as money or value transfer service (MVTs) providers rely on agents to undertake transactions, collecting and transferring funds from a customer and paying out funds to a beneficiary. Agents are also relied on for record keeping, reporting SARs or PTRs. While the general law of agency likely applies allowing businesses to use agents for functions other than CDD, this is not clearly stated in the Act. There is an additional question whether it is appropriate to use agents in every circumstance.



We consider some measures we could introduce to address the risks of money or value transfer service providers using agents to carry out their business. These are discussed below at page 77.



- 3.18. Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for?
- 3.19. Do you currently take any steps to ensure that only appropriate persons are able to act as your agent? What are those steps and why do you take them?
- 3.20. Should there be any additional measures in place to regulate the use of agents and third parties? For example, should we set out who can be an agent and in what circumstances they can be relied upon?

Offences and penalties

A comprehensive and effective offence and penalty regime is necessary for ensuring good regulatory outcomes and that businesses comply with their obligations. Supervisors need to be able to respond to non-compliance when it is detected, and impose penalties that are proportionate and dissuasive to influence decision making within businesses. In particular, enforcement action should support compliance, and not be factored into the cost of doing business for non-compliant businesses.

Recommended action (b) for Immediate Outcome 3 (page 118)

Sanctions available to AML/CFT supervisors should be enhanced to ensure there is a sufficient range of proportionate and dissuasive sanctions. This should include increasing the range of pecuniary penalties for non-compliance and providing AML/CFT supervisors with powers to impose administrative sanctions.

Comprehensiveness of penalty regime

The Act allows for a range of penalties to be imposed for non-compliance. Supervisors can impose a range of civil sanctions, including issuing formal warnings, accepting enforceable undertakings, seeking injunctions from the High Court, and applying for pecuniary penalties. In addition, businesses which knowingly or recklessly engage in non-compliance can be prosecuted and held criminally liable.

Overall, the supervisors make use of the full range of sanctions and penalties available in the Act, but primarily make use of public or private formal warnings in most cases of non-compliance, with enforceable undertakings and High Court injunctions seldomly used. In addition, pecuniary penalties can only be imposed following a resource-intensive court process and the ultimate penalties imposed may not be in proportion to the seriousness of the breaches.

Allowing for intermediary enforcement options

The Act currently does not provide a full range of potential interventions to AML/CFT supervisors which reflect the differing degrees of harm caused by non-compliance. In particular, supervisors may not be able to respond to moderately serious non-compliance – conduct that is more serious than a formal warning, but not sufficiently serious to require an injunction or pecuniary penalties.

We would like to explore what other options could be included to appropriately respond to non-compliance. One option is to allow AML/CFT supervisors to issue infringement notices and fines for straightforward misconduct (e.g. failing to file an annual report on time). 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.¹⁶

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. However, allowing administrative penalties to be imposed for AML/CFT breaches in all circumstances would require careful consideration of how these penalties coexist with the existing administrative tools.

¹⁶ Administrative penalties can currently be imposed in some circumstances (e.g. FMA can take action in relation to licensing in certain circumstances where there are AML/CFT breaches), but not in all circumstances and not by all supervisors.



- 3.21. Does the existing penalty framework in the AML/CFT Act allow for effective, proportionate, and dissuasive sanctions to be applied in all circumstances, including for larger entities? Why or why not?
- 3.22. Would additional enforcement interventions, such as fines for non-compliance or enabling the restriction, suspension, or removal of a licence or registration enable more proportionate, effective, and responsive enforcement?
- 3.23. Are there any other changes we could make to enhance the penalty framework in the Act?

Allowing for higher penalties at the top end of seriousness

The Act provides for civil pecuniary penalties and criminal penalties for serious non-compliance. Businesses which breach their obligations in a continuous or serious manner can face penalties of up to NZD 2 million for civil penalties and up to NZD 5 million for criminal penalties. However, while these penalties are large in the New Zealand context, they may not be sufficiently proportionate or dissuasive for large businesses, including branches of multinational companies. We want to explore whether the penalty range should be changed, and if so, how.



- 3.24. Should the Act allow for higher penalties at the top end of seriousness to ensure sufficiently dissuasive penalties can be imposed for large businesses? If so, what should the penalties be?

Sanctions for employees, directors, and senior management

The penalties in the Act can only apply to businesses themselves and not their directors or senior management. Ultimately the directors or senior managers are responsible for making decisions about how the business operates and whether it complies with the AML/CFT obligations. The FATF considers availability of such penalties to be a core component of an effective, proportionate, and dissuasive penalty regime.

We would like to explore whether enforcement and penalties, particularly civil penalties, should be able to be applied to directors and senior managers. This could ensure that the people who make compliance decisions are held responsible when instances of non-compliance occur. It would also avoid penalties being factored into the cost of doing business or being paid indirectly by a business' shareholders and/or customers.

If we enabled penalties to be imposed against directors, senior managers, or employees, we would also need to consider whether compliance officers can be held responsible. Compliance officers have statutory obligations to administer and maintain a business' AML/CFT programme, however, they may not be responsible for the business' decisions. In addition, compliance officers could be provided protections when acting in good faith, for example when they provide appropriate advice for how to comply which is ignored by senior managers and directors.



- 3.25. Would broadening the scope of civil sanctions to include directors and senior management support compliance outcomes? Should this include other employees?
- 3.26. If penalties could apply to senior managers and directors, what is the appropriate penalty amount?
- 3.27. Should compliance officers also be subject to sanctions or provided protection from sanctions when acting in good faith?

Liquidation following non-payment of AML/CFT Penalties

RBNZ and FMA are specifically empowered by the Companies Act 1993 to apply to a court for liquidation to recover pecuniary penalties on behalf of the Crown. There are no current provisions allowing DIA to similarly apply for liquidation for recovery of pecuniary penalties. The absence of a power to apply to a court prevents DIA from pursuing liquidation and fully enforcing compliance with the AML/CFT Act where pecuniary penalties are awarded against a business. Clarifying that all supervisors are able to apply to the court for liquidation of a business to recover pecuniary penalties awarded to the Crown would ensure consistency of enforcement.



- 3.28. 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?

Time limit for prosecuting AML/CFT offences

Sections 99 and 104 of the Act set out that the limitation period for prosecuting an AML/CFT offence is three years after the date on which the offence was committed. While this is in line with the potential penalty of two years imprisonment, it does risk some conduct going unpunished because too much time has elapsed. There can be a significant delay between when the wrongdoing occurs and supervisors identifying the potential criminal activity. A longer limitation period for prosecution would address this risk.



- 3.29. Should we change the time limit by which prosecutions must be brought by? If so, what should we change the time limit to?

Preventive measures

This section deals with the obligations that businesses have to prevent or mitigate the risk they are misused for money laundering and terrorism financing. The FATF's Recommendations set out appropriate preventative measures (particularly Recommendations 9 to 23). Effective preventive measures should be informed by and reflect an understanding of money laundering and terrorism financing risks and ultimately protect businesses from harm. However, AML/CFT obligations also impose significant and sometimes disproportionate compliance costs on businesses, particularly where they are not imposed in an efficient way or do not allow for innovative approaches to be taken.

Guiding questions for this section:

- Do the various obligations imposed by the Act enable businesses to adequately reduce their exposure to money laundering and terrorism financing? Are there any additional obligations that are needed? Are there any obligations that should be removed or amended because they are ineffective or unclear?
- How can we ensure compliance costs are proportionate to the nature of the money laundering and terrorism financing risks being avoided or mitigated and the size of the business?
- Can we improve efficiencies and better enable innovation within the regime?
- Are there any additional measures or steps that businesses are taking that are not required by the Act but are required by parent entities or relationships with other businesses (correspondent or otherwise)?

Customer due diligence¹⁷

Customer due diligence (CDD) is the foundation of an effective AML/CFT system. Knowing who a customer is, verifying any information provided and understanding their risk profile protects businesses from misuse. Developing a clear understanding of why a customer is forming a particular relationship also enables businesses to properly detect unusual or potentially suspicious behaviour.

This section looks at our general CDD settings including how the Act defines “customer” and what information the Act requires to be collected and verified, including on an ongoing basis. We also look at how businesses should approach situations of higher and lower risk and enhance or simplify CDD as appropriate.

¹⁷ New Zealand was rated largely compliant in our Mutual Evaluation for Recommendation 10, which relates to customer due diligence. This rating indicates that minor deficiencies exist in our legal framework. The main deficiencies identified relate to our beneficial ownership requirements, as well as having insufficient requirements for existing customers and enhanced CDD. We also do not have the comprehensive requirements to understand the nature of a customer's business and identify the powers that regulate and bind legal persons and arrangements, nor do we permit businesses to not pursue CDD where it may tip off the customer.

The core components of an effective obligation to conduct CDD involves clearly defining:

- **who** should be considered a customer;
- **when** various levels of CDD (standard, simplified, enhanced, and ongoing) should be conducted;
- **what** information should be obtained for each level of CDD;
- **how** the beneficial owner of a customer should be identified, including who should be considered a beneficial owner; and
- **how** information obtained as part of CDD should be verified.

In addition, we should ensure that enhanced and simplified CDD obligations are in line with higher and lower risks, that ongoing CDD and account monitoring obligations ensure customer information is up-to-date and that suspicions can be identified, and that we minimise the potential for inadvertently tipping off people when suspicions are formed.



4.1. What challenges do you have with complying with your CDD obligations? How could these challenges be resolved?

Definition of a customer

To conduct CDD, businesses must first identify the person – legal or natural – who is the ‘customer’. Customer is defined in [section 5](#) of the Act. However, businesses can sometimes have difficulties identifying the customer in some situations, particularly where the relationship or activity is complex, which can make conducting with CDD requirements challenging. Some examples include:

- identifying who is a customer when providing the service of ‘forming legal persons or legal arrangements’, as the legal person or arrangement does not exist before it is formed and therefore cannot be a customer;
- business relationships with trusts and other legal arrangements are inherently challenging, as legal arrangements by definition do not have legal personality (e.g. the trustees are listed as the owners of trust assets);¹⁸
- transferring money between parties can be confusing when a business has an ongoing relationship with both parties (e.g. a consumer and an ultimate merchant), as it could suggest that a business has two customers for the same activity;
- it is unclear what obligations DNFBPs have in respect of a third party when holding their funds in their trust account for the ultimate benefit of their customer (e.g. receiving deposits for a commercial transaction from prospective purchasers) .

We want to explore whether the more prescription is required as to who a customer is in various circumstances. This would provide businesses with more certainty, and would be in line with the approach that other countries take, [such as Australia](#). This may reduce compliance costs for

¹⁸ The AML/CFT supervisors have issued an [interpretative note](#) and [guidance](#) which treats the trust itself as a customer, even though trusts do not have legal personality.

some businesses, particularly where the current law unintentionally appears to require CDD to be performed on multiple parties.

- 4.2. Have you experienced any situations where trying to identify the customer can be challenging or not straightforward? What were those situations and why was it challenging?
- 4.3. Would a more prescriptive approach to the definition of a customer be helpful? For example, should we issue regulations to define who the customer is in various circumstances and when various services are provided?
- 4.4. If so, what are the situations where more prescription is required to define the customer?
- 4.5. Do you anticipate that there would be any benefits or additional challenges from a more prescriptive approach being taken?



Definition of a customer in real estate transactions

Real estate agents are required to comply with the full range of AML/CFT obligations when they represent either a purchaser, or a seller, in the purchase or sale of real estate. This means that real estate agents are required to carry out CDD on their customer but not the other party to the transaction.

The current requirements for real estate agents when conducting CDD are not in line with the FATF standards. The FATF requires real estate agents to conduct CDD on both the vendors and purchasers of the property. This approach may also be inconsistent with the risks associated with real estate transactions, given how attractive real estate is for criminals. Real estate is commonly restrained by Police and can be a straightforward way for dirty money to be reintegrated back into the legitimate economy and appear legitimate. Real estate also has the capacity to deliver capital gains as well as increase the complexity of the money laundering transaction.


In addition, it is typically the purchaser, rather than the vendor, who represents the main threat of money laundering or terrorism financing in real estate transactions. The current approach may also provide limited visibility over who initially pays the deposit, especially where they do not end up being the ultimate owner of the property.

We can amend the regulation which defines a real estate agent's customer to require CDD on both the purchaser and the vendor. This change would better recognise the risks associated with real estate transactions and align with FATF requirements. However, requiring real estate agents to conduct CDD on both parties potentially doubles the compliance costs associated with CDD.

Time at which real estate agents must conduct CDD

Currently, real estate agents must conduct CDD at the time the real estate agent enters into an agency agreement with their customer. We would need to carefully set the point at which CDD needed to be conducted if regulations required real estate agents to conduct CDD on both parties. Currently, real estate agents must conduct CDD at the time the real estate agent enters into an agency agreement with their customer. This does not account for the complexity of real estate agency relationships, including conjunctural arrangements, and also would not be appropriate for the purchaser (with whom no agreement is entered into). In addition, it is possible


for a nominee to engage with the real estate agent on behalf of the purchaser, with the agent only having visibility of the actual purchaser late in the process.

| | |
|--|---|
| <p>4.6. Should we amend the existing regulations to require real estate agents to conduct CDD on both the purchaser and vendor?</p> <p>4.7. What challenges do you anticipate would occur if this was required? How might these be addressed? What do you estimate would be the costs of the change?</p> <p>4.8. When is the appropriate time for CDD on the vendor and purchaser to be conducted in real estate transactions?</p> |  |
|--|---|

When CDD must be conducted

Section 11 of the Act sets out that a business must conduct customer due diligence on a customer, any beneficial owner of a customer, and any person acting on behalf of a customer.

- **Standard CDD** is required for new customers, occasional transactions, occasional activities, and for some existing (pre-Act) customers where there has been a material change in the nature or purpose of the business relationship and the business considers it has insufficient information about the customer.
- **Simplified CDD** can be conducted for business relationships, occasional transactions, and occasional activities with specific types of low-risk customers, as well as for persons acting on behalf of a customer who has already been subject to CDD.
- **Enhanced CDD** must be conducted where the risk is elevated for a variety of reasons, including if the customer is a trust, politically exposed person, seeks to conduct a complex, unusually large transaction or pattern of transactions, or where a SAR has been filed.

| | |
|---|---|
|  | <p>4.9. Are the prescribed points where CDD must be conducted clear and appropriate? If not, how could we improve them?</p> <p>4.10. For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear?</p> |
|---|---|

Conducting customer due diligence in all suspicious circumstances

Currently, there is no requirement under the Act for a business to conduct CDD if suspicious transactions occur outside of a business relationship and the amounts involved do not meet the threshold for an occasional transaction. This is not in line with the FATF standards, which require CDD whenever there is a suspicion of money laundering or terrorism financing regardless of any exemptions or thresholds that are in place. Requiring CDD in all situations of suspicion would enhance the ability of the regime to detect and deter money laundering, including where suspicious transactions are typically of low value (e.g. terrorism financing or payments for online child exploitation).

However, we would need to carefully consider how any obligation would work in practice given the absence of a business or customer relationship with the person concerned. This change would also potentially increase costs for businesses, depending on the level of CDD and what

verification was required. We would also need to ensure the requirement does not lead to businesses inadvertently tipping off the person by conducting CDD (we discuss tipping off in the CDD context at page 65, below).

- 4.11. Should CDD be required in all instances where suspicions arise?
- 4.12. If so, what level of CDD should be required, and what should be the requirements regarding verification? Is there any information that businesses should not need to obtain or verify?
- 4.13. How can we ensure that this obligation does not put businesses in a position where they are likely to tip off the person?



Managing funds in trust accounts

There are significant risks and vulnerabilities associated with trust accounts, and we want to explore whether more needs to be done to mitigate these risks. We also want to understand whether the vulnerabilities associated with trust accounts are unique to law firms, or whether they also apply to accounting practices, real estate agents or TCSPs that hold funds in trust accounts.

We could potentially issue regulations to introduce further requirements or controls in relation to the use of trust accounts (e.g. requiring CDD before refunding money to a third party). We could also limit any additional controls to only apply in certain situations, such as if the value of funds received does not align with instructions or is more than expected. Introducing further controls would potentially mitigate the risks and vulnerabilities we have identified; however, they would also increase compliance costs for affected businesses.

- 4.14. What money laundering risks are you seeing in relation to law firm trust accounts?
- 4.15. Are there any specific AML/CFT requirements or controls that could be put in place to mitigate the risks? If so, what types of circumstances or transactions should they apply to and what should the AML/CFT requirements be?
- 4.16. Should this only apply to law firm trust accounts or to any DNFBP that holds funds in its trust account?
- 4.17. What do you estimate would be the costs of any additional controls you have identified?



What information needs to be obtained and verified

The Act prescribes a different amount of information that needs to be obtained and verified depending on the level of CDD conducted:

- **Standard CDD** requires businesses to obtain and verify a variety of basic information, such as the person's name, date of birth, address or registered office, company identifier or registration number, their relationship to the customer (if they are not the customer), and obtain enough information to determine whether the person should be subject to enhanced CDD.

- **Simplified CDD** only requires businesses to obtain and verify a person's full name, date of birth, and relationship to the customer if they are acting on behalf of a prescribed low-risk customer type.
- **Enhanced CDD** requires businesses to obtain and verify the information required by standard CDD as well as, in most instances, information about the source of wealth or source of funds of the customer and information about any beneficiaries if the customer is a trust.

In addition, irrespective of the level of CDD, all businesses are required to obtain information about the nature and purpose of the proposed business relationship with the customer.



- 4.18. Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?
- 4.19. Are the obligations to obtain and verify information clear?
- 4.20. Is the information that businesses should obtain and verify about their customers still appropriate?
- 4.21. Is there any other information that the Act should require businesses to obtain or verify as part of CDD to better identify and manage a customer's risks?

Obligations for legal persons and legal arrangements

The FATF standards require businesses to obtain and verify specific information about customers which are legal persons or legal arrangements to better understand their customer, how they operate, and any risks they may present.

In particular, the FATF standards require businesses to obtain and verify information about the customer's legal form and proof of existence, ownership and control structure, and powers that bind and regulate (e.g. voting rights which attach to categories of shares and founding documents which set out how the legal person or arrangement can operate).

Businesses are already required to obtain a customer's registration number (which could indicate the legal form) but not whether the customer is still incorporated. A registration number also cannot be relied on to determine whether a legal arrangement exists, as legal arrangements typically do not have registration numbers. Explicitly requiring proof of existence will help protect businesses from opening accounts for legal persons which no longer exist.

In addition, requiring businesses to understand the ownership and control structure and powers that bind and regulate the person or arrangement would help them understand the business relationship and assess the customer's risk profile. It could also help identify beneficial owners of the customer, particularly third parties that are not owners or direct controllers but nonetheless exert influence over how the legal person or arrangement operates.

We can issue regulations to explicitly require businesses to obtain this information as part of standard CDD, which would ensure we are aligned with the FATF standards. However, we are conscious that any change to CDD can increase compliance costs. If we required businesses to obtain this information, we would also need to consider how this information is verified as there may not be an independent source that can be relied on for some information.

- 4.22. Should we issue regulations to require businesses to obtain and verify information about a legal person or legal arrangement's form and proof of existence, ownership and control structure, and powers that bind and regulate? Why?
- 4.23. Do you already obtain some or all of this information, even though it is not explicitly required? If so, what information do you already obtain and why?
- 4.24. What do you estimate would be the impact on your compliance costs for your business if regulations explicitly required this information to be obtained and verified?



Source of wealth versus source of funds

Businesses are required to obtain and verify information about the customer's source of wealth or source of funds when enhanced CDD is triggered under [section 22\(1\)](#). However, the Act does not specify when source of wealth should be identified versus the source of funds. In particular, the Act does not make it clear that source of funds should be examined when enhanced CDD is triggered due to a particular transaction that is assessed as high risk.

We can issue regulations to prescribe specific circumstances in which source of wealth or source of funds, or both, are required. The AML/CFT supervisors [have issued guidance](#) clarifying how 'wealth' and 'funds' interact with each other, and when it may be necessary to identify and verify one versus the other. Issuing regulations would provide further clarity to businesses and ensure that enhanced CDD measures address money laundering and terrorism financing risks.

- 4.25. Should we issue regulations to prescribe when information about a customer's source of wealth should be obtained and verified versus source of funds? If so, what should the requirements be for businesses?
- 4.26. Are there any instances where businesses should not be required to obtain this information? Are there any circumstances when source of funds *and* source of wealth should be obtained and verified?
- 4.27. Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds?



Beneficiaries of life and other investment-related insurance

Some insurance policies, particularly life insurance or other investment related insurance policies that allow for early surrenders or withdrawals, have been identified internationally as being potentially risky for money laundering or terrorism financing. When dealing with these potentially risky insurance policies, the FATF standards require businesses to obtain the name of any beneficiaries or classes of beneficiaries. In addition, the beneficiary should be considered as a relevant risk factor when determining what level of CDD to conduct.

We can issue regulations to bring New Zealand in line with the FATF standards. while we understand that no life insurers in New Zealand currently offer any policies that are potentially

risky, there is still the potential for New Zealand businesses to be exposed to these risks, including if insurers begin to offer these products in the future.

However, we would want to ensure that we do not unnecessarily increase compliance obligations in an area which is currently lower risk. One option could be to only require this information to be obtained for insurance policies which we identify as representing moderate or high risks in line with FATF guidance for a risk-based approach to the life insurance sector.¹⁹ This would not impose any additional obligations on life insurers unless they started issuing risky policies.

- 4.28. Should we issue regulations to require businesses to obtain information about the beneficiary/ies of a life insurance or investment-related insurance policy and prescribe the beneficiary/ies as a relevant risk factor when determining the appropriate level of CDD to conduct? Why or why not?
- 4.29. If we required this approach to be taken regarding beneficiaries of life and other investment-related insurance policies, should the obligations only apply for moderate or high-risk insurance policies? Are there any other steps we could take to ensure compliance costs are proportionate to risks?



Identifying the beneficial owner

Identifying and verifying the person who ultimately owns or controls a customer is key to ensuring that businesses are not misused for money laundering or terrorism financing. Criminals and terrorists can use legal persons and legal arrangements to obscure their involvement and gain access to the formal financial system when they otherwise may not be able to.

New Zealand legal persons and arrangements are attractive to criminals, given our strong international reputation for low corruption, high integrity, and ease of doing business. As such, it is important that the beneficial ownership obligations in the Act protect our businesses from misuse. Our risks and vulnerabilities will also increase as more countries implement stronger measures to ensure transparency of beneficial ownership, as we will end up lagging behind our international peers.

Definition of beneficial owner

A beneficial owner is defined in the Act as the individual who (a) has effective control of a customer or person on whose behalf a transaction is conducted; or (b) owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted. We have identified several different issues with the definition of beneficial owner which could be resolved, but we are also interested in how else we can improve our definition to make it clear and easy to understand and apply, including whether the Beneficial Ownership Guidelines need to be amended.

¹⁹ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf>. Higher risk policies include products with the potential for multiple investment accounts and/or products with returns linked to the performance of an underlying financial asset, or products designed for high net worth persons



- 4.30. Have you encountered issues with the definition of a beneficial owner? If so, what about the definition was unclear or problematic?
- 4.31. How can we improve the definition in the Act as well as in guidance to address those challenges?

'Ultimate' ownership and control

The definition in the Act does not include concepts of 'ultimate' ownership or control, which is intended to refer to situations where ownership or control is exercised through a chain of ownership or by indirect means of control. As such, our definition is inconsistent with the FATF standards and could mean that businesses may stop at the first ownership or control layer and look no further.

In practice, the Beneficial Ownership Guidelines issued by the three AML/CFT supervisors address this issue by making it clear that businesses should be identifying ultimate ownership and control. However, guidance cannot be enforced. We could issue an "avoidance of doubt" regulation which states that the focus should be on identifying the 'ultimate' beneficial owner. This would provide further clarity to businesses about their obligations, but may increase compliance costs, particularly if businesses are stopping at the first ownership or control layer and not looking further.

- 4.32. Should we issue a regulation which states that businesses should be focusing on identifying the 'ultimate' beneficial owner? If so, how could "ultimate" beneficial owner be defined?
- 4.33. To extent are you focusing beneficial ownership checks on the 'ultimate' beneficial owner, even though it is not strictly required?
- 4.34. Would there be any additional costs resulting from prescribing that businesses should focus on the 'ultimate' beneficial owner?



The 'person on whose behalf a transaction is conducted'

The Act includes "the person on whose behalf a transaction is conducted" in both limbs of the definition of beneficial owner. Not only is this inconsistent with the FATF's standards and guidance,²⁰ the AML/CFT supervisors have issued guidance which interprets this person as a third 'type' of beneficial ownership.

Some businesses have customers in turn transact on behalf of their own underlying customers. As a result of how the definition has been interpreted, businesses in this position have been

²⁰ The FATF notes that the inclusion of the natural persons on whose behalf a transaction is conducted, even where that person does not have actual or legal ownership or control over the customer: "this element of the FATF definition of beneficial owner focuses on individuals that are central to a transaction being conducted even where the transaction has been deliberately structured to avoid control or ownership of the customer but to retain the benefit of the transaction." (FATF, Transparency and Beneficial Ownership Guidance, page 8)

required to treat the customer of a customer as a beneficial owner and obtain and verify the underlying customer's identity.²¹

We could issue a regulation to clarify what is meant by the “person on whose behalf a transaction is conducted” in the definition of beneficial owner. In line with the FATF’s guidance, this regulation could state that transactions being conducted on behalf of another person are only relevant when they imply that the other person is exercising indirect ownership or control. This would clarify the obligation and ensure that businesses do not have a direct obligation to obtain and verify the identity of every underlying customer of their customer.²² If we provided this clarification, we would also likely recommend revoking the current “specified managing intermediaries” exemption and Regulation 24 of the AML/CFT (Exemptions) Regulations 2011 as they would be unnecessary.

- 4.35. Should we issue a regulation which states that for the purposes of the definition of beneficial owner, a person on whose behalf a transaction is conducted is restricted to a person with indirect ownership or control of the customer (to align with the FATF standards)? Why or why not?
- 4.36. Would this change make the “specified managing intermediaries” exemption or Regulation 24 of the AML/CFT (Exemption) Regulations 2011 unnecessary? If so, should the exemptions be revoked?
- 4.37. Would there be any additional compliance costs or other consequences for your business from this change? If so, what steps could be taken to minimise these costs or other consequences?



Process for identifying who ultimately owns or controls legal persons

The FATF standards set out that businesses should identify who ultimately owns or controls a legal person through the following process:

- **Step 1:** identify any natural persons (if any, as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person through ownership) who ultimately have a controlling ownership interest in a legal person.
- **Step 2:** to the extent there is any doubt under Step 1 as to whether the person(s) with the controlling interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, identify natural persons (if any) exercising control of the legal person through other means.
- **Step 3:** where no natural person is identified through Steps 1 or 2, the business should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

²¹ Regulations have exempted businesses from this obligation in relation to trust accounts or client funds account and where businesses are licensed or specified managing intermediaries.

²² We note that this does not preclude a business from a requirement to obtain and verify the identity of an underlying customer of its customer for some circumstances and transactions. However, in accordance with a risk based approach, if we issued the proposed clarification, this would only arise when enhanced CDD was triggered. In these circumstances the reason for identifying the underlying person would be because they are (part of) the source of funds or wealth of the customer (but not because they are a beneficial owner).

The *Beneficial Ownership Guideline* issued by the three AML/CFT supervisors is mostly, but not entirely, in line with FATF standards. One difference is the relevance of considering whether a person on whose behalf a transaction is being conducted is a beneficial owner (discussed above). The other key difference is that the guidance does not state that senior managing official should be treated as a beneficial owner where no person can be identified who owns or controls the legal person.

We could issue regulations or a Code of Practice which mandates an approach consistent with FATF standards for identifying the beneficial owner of a legal person. This could include stating that a senior managing official should be identified as the beneficial owner where no persons can otherwise be identified. This change would provide further clarity to businesses as to the process they should follow. It may increase compliance costs for businesses which do not follow the existing guidance but may also reduce compliance costs for businesses when they cannot identify a beneficial owner by allowing senior managing officials to be identified for this purpose.

- 4.38. What process do you currently follow to identify who ultimately owns or controls a legal person, and to what extent is it consistent with the process set out in the FATF standards?
- 4.39. Should we issue regulations or a Code of Practice which is consistent with the FATF standards for identifying the beneficial owner of a legal person?
- 4.40. Are there any aspects of the process the FATF has identified that not appropriate for New Zealand businesses?
- 4.41. Would there be an impact on your compliance costs by mandating this process? If so, what would be the impact?



Process for identifying who ultimately owns or controls legal arrangements

As with legal persons, the FATF recommends that businesses should obtain information about specific persons who may be involved in the operation of a legal arrangement. In particular, best practice is to identify and verify the settlor, trustee, and protector of a trust, and equivalent positions in other legal arrangements. The Act does not explicitly require businesses to identify all these classes of people, although some people might be identified through enhanced CDD (e.g. the settlor might be identified as a result of identifying the source of wealth or funds).

We can issue regulations and/or a Code of Practice to require information about these persons to be obtained as part of standard CDD when the customer is a legal arrangement. This would ensure that businesses are properly identifying all persons who may be in a position to influence how the legal arrangement operates and determine who the beneficial owner is. However, it would also require businesses to obtain additional information which can increase compliance costs.

- 4.42. Should we issue regulations or a Code of Practice that allows businesses to satisfy their beneficial ownership obligations by identifying the settlor, the trustee(s), the protector and any other person exercising ultimate effective control over the trust or legal arrangement?



4.43. Would there be an impact on your compliance costs by mandating that this process be applied? If so, what is the impact?

Reasonable steps to verify information obtained through CDD

The Act requires reasonable steps to be taken to verify information obtained about the customer and beneficial owner(s) through CDD. This requirement is intended to ensure that the information is correct: money launderers and terrorist financiers want to remain anonymous and providing false information and fraudulently opening accounts is an easy way to achieve anonymity.

The Act prescribes different standards of verification depending on whether the information is about the customer, the beneficial owner, or the person acting on behalf of a customer. For example, businesses should take reasonable steps to satisfy itself that the information about the customer “is correct”, whereas businesses are required to take reasonable steps (according to the level of risk involved) to verify a beneficial owner’s identity so that the business is “satisfied that it knows who the beneficial owner is.” In addition, the Act prescribes that verifying identity must be done on the basis of documents, data, or information issued by a reliable and independent source.



4.44. Are the standards of verification and the basis by which verification of identity must be done clear and still appropriate? If not, how could they be improved?

Identity Verification Code of Practice

The AML/CFT supervisors have issued an [Identity Verification Code of Practice](#) (IVCOP) to provide suggested best practice (and a safe harbour) for businesses when verifying the name and date of birth of customers (who are natural persons), or other persons requiring CDD, that have been assessed to be low to medium risk. In particular, IVCOP sets out what documents can be relied upon to verify identity, how many documents must be sighted, how document certification should occur, and sets out the steps to verify information electronically.

We want to ensure that IVCOP is as comprehensive as possible to ensure that businesses are clear about their CDD obligations in all circumstances and that a consistent approach is taken across all sectors. We have identified the following gaps or challenges with IVCOP:

- best practice is not identified for higher risk customers, customers who are legal persons or legal arrangements, or international customers.
- some forms of identification that might be reliable are not included in IVCOP (e.g. an Australian driver licence).
- there are no standards for biometric verification, ongoing CDD, and when CDD is shared between businesses (e.g. as part of a DBG).
- the current requirements for electronic verification may not be fit-for purpose, particularly as more businesses move to online-only interactions with their customers

Providing further clarity or identifying additional best practices also has the potential to alleviate compliance challenges and reduce compliance costs.

- 4.45. Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?
- 4.46. Is the approach in IVCOP clear and appropriate? If not, why?
- 4.47. Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g. verifying name and date of birth of high-risk customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?
- 4.48. Are there any identity documents or other forms of identity verification that businesses should be able to use to verify a customer's identity?
- 4.49. Do you have any challenges in complying with Part 3 of IVCOP in relation to electronic verification? What are those challenges and how could we address them?



Verifying the address of customers who are natural persons

The Act requires businesses to obtain and verify address information for all customers, beneficial owners and persons acting on behalf of a customer. Address verification was included as a measure to ensure accuracy of a person's identity information as well as further enabling the ability for transactions to be traced around the economy and thereby support law enforcement outcomes.

Most countries do not require address information to be verified, although some countries have alternative means for confirming a person's address (e.g. some form of national identification card and household registration). Requiring verification may have some deterrent effect and can carry more weight in some law enforcement applications, such as applying for a warrant. Nevertheless, we have identified a number of issues with this requirement:

- **it can negatively impact financial inclusion, particularly for vulnerable populations:** some customers may not be able to provide evidence of an address to be verified for a variety of reasons, including that they do not have permanent accommodation, or they are not the account holder for any utility bills. In addition, people often do not have easy access to suitable documentation which proves their address which can unnecessarily extend the time it can take to establish a business relationship and open an account.
- **it can result in disproportionate compliance costs for businesses:** CDD quality assurance processes within businesses commonly identify faults with address verification which require fixing. Fixing these issues require staff to contact the customer and reobtain proof of address, which can be a time-consuming process.
- **current processes for verifying address are not robust:** a common method for verifying address information is to rely on statements issued from a financial institution, such as a bank. However, most financial institutions allow for customers to easily update their address information and typically do not reverify the new address information. Any statements issued with the updated address information do not prove that the information is correct but are relied on for that purpose.

- **it goes beyond the FATF standards**, which only require address information to be verified when the customer is a legal person or legal arrangement and when a person conducts an international wire transfer.

There are a number of ways we could resolve these challenges:

- in the short term, we could issue regulations to only require address verification to occur for higher risk customers that are natural persons. We could also amend IVCOP to include how businesses should verify address information to ensure a consistent and robust approach. We could also change the basis for verifying address information and enable verification through other means, such as businesses sending their customer a letter.
- In the long term, we could amend the requirement in the Act itself to still require address information to be obtained, but only verified in instances where it is valuable to do so (e.g. as part of a wire transfer or when suspicions are raised)

- 4.50. What challenges have you faced with verification of address information? What have been the impacts of those challenges?
- 4.51. In your view, when should address information be verified, and should that verification occur?
- 4.52. How could we address challenges with address verification while also ensuring law enforcement outcomes are not undermined? Are there any fixes we could make in the short term?



Obligations in situations of higher and lower risk

Expanding the range of measures available to mitigate high-risk customers

Enhanced CDD should be applied in situations of higher risk and is intended to mitigate risks identified by requiring businesses to take additional steps as part of CDD. Our Act generally only requires two additional steps to be taken: obtain information about the source of wealth or source of funds and obtain information about the beneficiaries of a customer which is a trust.²³ This is not consistent with the FATF standards, which identifies a range of other measures that businesses could take to manage and mitigate higher risk situations, including:

- obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- obtaining additional information on the intended nature of the business relationship.
- obtaining information on the reasons for intended or performed transactions.
- obtaining the approval of senior management to commence or continue the business relationship.

²³ There are additional steps that need to be taken for customers who are politically exposed persons ([section 26](#)), where wire transfers are conducted ([section 27](#) to [28](#)), where a business seeks to form a correspondent banking relationship ([section 29](#)), or where new or developing technologies or that might favour anonymity are involved ([section 30](#)).

- conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

We could issue regulations or a Code of Practice which requires businesses to consider applying these additional measures when faced with situations of higher risk. This would align our law with the FATF standards and clearly signal to businesses what other measures they can take to manage, rather than avoid, situations where there are higher risks. However, we would need to think carefully about whether and in what circumstances any of these additional measures are mandatory as this would directly impact compliance costs. For example, businesses could be mandated to conduct one or a number of the additional measures (depending on the circumstances) or conduct certain measures in certain circumstances.

- 4.53. Do you currently take any of the steps identified by the FATF standards to manage high-risk customers, transactions or activities? If so, what steps do you take and why?
- 4.54. Should we issue regulations or a Code of Practice which outlines the additional measures that businesses can take as part of enhanced CDD?
- 4.55. Should any of the additional measures be mandatory? If so, how should they be mandated, and in what circumstances?



Conducting simplified CDD on persons acting on behalf of large organisations

The Act requires business to verify the identity and authority of any person acting on behalf of a customer. While these requirements are important and not an issue to apply in most circumstances, they can be challenging where the customer is a large organisation and there may be many authorised persons at any one time.

We are interested in views as to how we could create more streamlined provisions for customers that are large organisations. For example, we could potentially issue regulations to allow employees to be delegated to act on behalf of the customer by a senior manager but without triggering CDD. This would ensure that the compliance burden of engaging with persons who act on behalf of a large organisation is in proportion to the risks identified.

- 4.56. Are there ways we can enhance or streamline the operation of the simplified CDD obligations, in particular where the customer is a large organisation?
- 4.57. Should we issue regulations to allow employees to be delegated by a senior manager without triggering CDD in each circumstance? Why?



Mandatory enhanced CDD for all trusts

Section 22 of the Act currently requires enhanced CDD for all customers who are trusts or another vehicle for holding personal assets. This is inconsistent with the FATF standards and inconsistent with the risk-based approach as not all trusts are inherently high risk.

We could remove the requirement that enhanced CDD be conducted for all trusts and rely on the requirement that enhanced CDD be conducted in high-risk situations. This would enable businesses to conduct standard CDD on trusts where there are no indicators of high risk but would require further guidance as to when a trust should be considered high risk. This would reduce compliance costs for businesses when dealing with trusts that are not high risk, and compliance costs for the trusts themselves. If we made this change, we could also specifically identify high risk categories of trusts which do require enhanced CDD to provide further clarity.



- 4.58. Should we remove the requirement for enhanced CDD to be conducted for all trusts or vehicles for holding personal assets? Why or why not?
- 4.59. If we removed this requirement, what further guidance would need to be provided to enable businesses to appropriately identify high risks trusts and conduct enhanced CDD?
- 4.60. Should high-risk categories of trusts which require enhanced CDD be identified in regulation or legislation? If so, what sorts of trusts would fall into this category?

Ongoing customer due diligence and account monitoring

Although CDD is required at the start of a business relationship, it is important to maintain this information as part of an ongoing process. Not only does this ensure that the business holds the most up-to-date information about the customer, it also ensures that their understanding of the customer's risk remains current. In addition, account monitoring allows businesses to identify any unusual patterns of behaviour or transaction, including where the customer's activity is not consistent with the nature and purpose of the business relationship.



- 4.61. Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?

Considering whether and when customer due diligence was last conducted

The Act does not require businesses to consider whether and when CDD was last conducted as part of ongoing CDD and account monitoring, nor are businesses required to consider the adequacy of the information previously obtained. This is a gap in our framework that presents a potential vulnerability for businesses as it does not ensure that customer information will be current or adequate. We could issue regulations to address this gap and explicitly require businesses to consider these factors when conducting ongoing CDD and account monitoring, including in relation to existing customers. However, this would likely increase compliance costs in the short term as ongoing CDD would likely be required in more circumstances.

- 4.62. As part of ongoing CDD and account monitoring, do you consider whether and when CDD was last conducted and the adequacy of the information previously obtained?
- 4.63. Should we issue regulations to require businesses to consider these factors when conducting ongoing CDD and account monitoring? Why?
- 4.64. What would be the impact on your compliance costs if we issued regulations to make this change? Would ongoing CDD be triggered more often?
- 4.65. Should we mandate any other requirements for ongoing CDD, e.g. frequently it needs to be conducted?



Ongoing CDD requirements where there are no financial transactions

The existing obligations for account monitoring and ongoing CDD require businesses to review “account activity and transaction behaviour”. For DNFBPs, transactions (as defined) may only be a small part of the activities within a business relationship with its customer, and in some circumstances, there may not be any financial transactions at all. In these circumstances, it is currently unclear when a DNFBP is required to undertake monitoring of the non-transaction-based activities of their customers, if at all. We can issue regulations requiring businesses to review any activities provided to the customer as part of ongoing CDD and account monitoring. This would ensure that DNFBPs have clear obligations which are equivalent to obligations for financial institutions.

- 4.66. If you are a DNFBP, how do you currently approach your ongoing CDD and account monitoring obligations where there are few or no financial transactions?
- 4.67. Should we issue regulations to require businesses to review activities provided to the customer as well as account activity and transaction behaviour? What reviews would you consider to be appropriate?
- 4.68. What would be the impact on your compliance costs if we issued regulations to make this change?



Information that needs to be reviewed for account monitoring

The Act only requires businesses to review the customer’s account activity and transaction behaviour. However, reviewing account activity or transactions may not be sufficient to identify suspicions in all circumstances or confirm that a customer is acting in accordance with the nature and purpose of the business relationship. Other information, such as the customer’s IP address, could be useful for identifying instances where a customer’s activity is inconsistent with their risk profile.

We want to explore whether we should issue regulations requiring businesses to review other information as part of account information, and if so, what additional information should be reviewed. This would ensure that businesses are considering all relevant information and potentially increase the likelihood of detecting suspicious or unusual activity. However, increasing

the amount of information that needs to be reviewed would increase compliance costs and not all information would be relevant to all businesses or customers.

- 4.69. Do you currently review other information beyond what is required in the Act as part of account monitoring? If so, what information do you review and why?
- 4.70. 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?



Conducting CDD on existing (pre-Act) customers

When the Act was originally passed in 2009, the government recognised that existing businesses would have a potentially large customer bases that had not been subjected to sufficient CDD. To address this concern, the Act requires CDD to be applied to existing customers according to the level of risk involved, where there has been a material change in the nature of the purpose of the business relationship and the business considers it has insufficient information about the customer. In addition, enhanced CDD would apply to the existing (pre-Act) customers and be triggered in instances of higher risks.

While this approach is largely in line with the FATF standards, we also recognise that some businesses may have still significant portions of their existing customer base which have not been subject to CDD. This represents a vulnerability for those businesses as well as for the overall system, and we want to explore how we can address this vulnerability.

Making the trigger an 'or' rather than an 'and'

Currently standard CDD is required when the business considers that it has both insufficient information and there has been a material change in the nature or purpose of the business relationship. We could change this so that standard CDD is required when there is insufficient information *or* there is a material change. This would mean that insufficient customer information alone would trigger CDD, irrespective of whether there is a material change in the nature or purpose of the business relationship.

Changing what is meant by a 'material change'

Our Act requires businesses to consider whether there is a 'material change to the nature or purpose of the business relationship' when deciding whether to conduct CDD on an existing customer. While it is a potentially high standard, it is intended to ensure that existing customers are subject to CDD over time and this is largely in line with the FATF standards.

To increase the likelihood that a business conducts CDD on an existing (pre-Act) customer, we could instead require CDD where a business becomes aware that the circumstances of an existing customer have changed (where those circumstances are relevant to the business's risk assessment). We could also remove 'material' from the trigger, such that any change to the business relationship could trigger CDD. Finally, we could also expand the scope of the trigger beyond the business relationship to also include any changes to the customer (including their beneficial owner).

Introducing a timeframe or ‘sinking lid’ for existing (pre-Act) customers

A more prescriptive option would be to introduce a timeframe or ‘sinking lid’ by which CDD on existing (pre-Act) customers must be conducted. A timeframe would mandate that all existing customers have to be subject to CDD by a certain date. By contrast, a ‘sinking lid’ approach would require businesses to progressively CDD parts of their existing customer base over time (e.g. CDD all customers where the business relationship was formed before 2000 one year, 2001 the next, and so forth).



- 4.71. How could we ensure that existing (pre-Act) customers are subject to the appropriate level of CDD? Are any of the options appropriate and are there any other options we have not identified? What would be the cost implications of the options?

Avoiding tipping off

The FATF standards require CDD to be performed in all instances of suspicion, and enhanced CDD where risks are higher. However, where suspicion is formed, the FATF standards allow for businesses to decline to conduct CDD where there is a risk that the process of conducting CDD will tip off the customer and file a SAR instead.

Our Act does not currently provide reporting entities with the discretion to apply lesser CDD measures to avoid tipping off, including not conducting CDD and filing a SAR instead. [Section 22\(1\)\(d\)](#) of the Act requires businesses to conduct enhanced CDD whenever the level of risk is such that enhanced CDD should apply. For an existing (pre-Act) customer and a person engaging in an occasional transaction or activity, [section 22A](#) of the Act also explicitly requires a business to conduct enhanced CDD as soon as practicable *after* becoming aware that a SAR must be reported.

Conducting enhanced CDD is a key part of being able to determine whether there are grounds to submit a SAR. However, we also acknowledge that conducting enhanced CDD could alert a customer that a business intends to submit a SAR and therefore tip them off that the business has formed suspicions and has, or will, file a SAR (particularly where [section 22A](#) is triggered). We also understand that for occasional transactions or activities, conducting enhanced CDD after the event may be extremely difficult in practice, and in turn so unusual that it may tip off the customer that the business intended to submit a SAR.

We want to explore whether more needs to be done to ensure businesses do not tip off customers by conducting CDD when suspicions have been formed. However, any efforts to resolve these challenges need to be balanced against ensuring the FIU receives quality intelligence as the quality of reporting may be undermined if a threshold for tipping off is set too low.



- 4.72. Should the Act set out what can constitute tipping off and set out a test for businesses to apply to determine whether conducting CDD or enhanced CDD may tip off a customer?
- 4.73. Once suspicion has been formed, should reporting entities have the discretion not to conduct enhanced CDD to avoid tipping off?

- 4.74. If so, in what circumstances should this apply? For example, should it apply only to business relationships (rather than occasional transactions or activities)? Or should it only apply to certain types of business relationships where the customer holds a facility for the customer (such as a bank account)?
- 4.75. Are there any other challenges with the existing requirements to conduct enhanced CDD as soon as practicable after becoming aware that a SAR must be reported? How could we address those challenges?

Record keeping²⁴

Effective and appropriate record keeping is key for an AML/CFT regime to operate effectively. The purpose of keeping records is three-fold: it should enable law enforcement authorities to reconstruct individual transactions so as to investigate and provide, if necessary, evidence for prosecution of criminal activity. It should also enable businesses to review and reconstruct a customer’s transaction history when undertaking ongoing CDD and account monitoring, and to report suspicious activity. Finally, it should provide a sufficient basis for supervisors to determine the extent to which a business is complying with their obligations, particularly CDD and account monitoring obligations.



- 4.76. Do you have any challenges with complying with your record keeping obligations? How could we address those challenges?
- 4.77. Are there any other records we should require businesses to keep, depending on the nature of their business?

Transactions outside a business relationship

Businesses are exempt from keeping records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold. The basis for this exemption is that the parties will not have been subject to CDD, so the business may not have the information about who the parties are in the first place. However, we are interested in whether this exemption hinders the ability for businesses to reconstruct transactions which occur outside a business relationship or below the occasional transaction threshold.

- 4.78. Does the exemption from keeping records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold hinder reconstruction of transactions? If so, should the exemption be modified or removed?



²⁴ New Zealand was rated largely compliant in our Mutual Evaluation for Recommendation 11, which relates to record keeping. This rating indicates that minor deficiencies exist in our legal framework. The deficiency identified is that our law does not specify a retention period for account files, business correspondence and written findings.

Politically exposed persons²⁵

New Zealand is generally considered to be a country with low levels of corruption, across both central and local government. We consistently rank at or near the top of Transparency International's *Corruption Perceptions Index*,²⁶ and we were at the top of the World Bank's Worldwide Governance Indicator relating to the control of corruption in 2019.²⁷

Politically exposed persons (PEPs) are people with significant control or influence within a government or international organisation. Our current settings for PEPs – which focus on addressing the risk of foreign PEPs rather than domestic PEPs – reflect the high level of integrity in New Zealand. However, even in high integrity environments, people with influence or control can be vulnerable to being targeted and corrupted by criminals or foreign influence. As such, and in line with our stewardship and international obligations, we need to review our current settings to ensure they are fit-for-purpose and will continue to keep New Zealand safe from corruption and foreign interference.

PEPs can be considered to be riskier customers, particularly where the PEP is from another country or has control over how a government spends its money. To ensure New Zealand businesses are protected from corruption and corrupt activity, we need to consider whether the Act properly protects against the risk that PEPs can pose, particularly PEPs from other countries.

The FATF expects countries to require businesses to take enhanced measures to ensure PEPs are not misusing their positions of authority. These measures include being able to determine whether a customer is a PEP and taking additional steps to mitigate the risks the PEP poses (such as obtaining senior management approval or a more detailed scrutiny of transactions). Ensuring that our obligations with respect to PEPs reflect our risk and context will help ensure our economy and public institutions are protected from misuse.



4.79. Do you have any challenges with complying with the obligations regarding politically exposed persons? How could we address those challenges?

4.80. Do you take any additional steps to mitigate the risks of PEPs that are not required by the Act? What are those steps and why do you take them?

²⁵ New Zealand was rated partially compliant in our Mutual Evaluation for Recommendation 12, which relates to politically exposed persons (PEPs). This rating indicates that moderate deficiencies exist in our legal framework. A key deficiency is that our definition of PEP has several issues, including that it does not cover domestic and international organisation PEPs. The Act also does not require businesses to obtain senior management approval before establishing a business relationship with a PEP or obtain information about the PEP's source of wealth or funds.

²⁶ Ranked first equal with Denmark in 2020: <https://www.transparency.org/en/cpi/2020/index/nzl>

²⁷ Across the six Worldwide Governance Indicators, New Zealand was ranked in 2019 as follows: voice and accountability – 5th; political stability and absence of violence/terrorism – 7th; government effectiveness – 13th; regulatory quality – 3rd; rule of law – 6th; control of corruption – 1st.
<https://info.worldbank.org/governance/wqi/Home/Reports>

Definition of a politically exposed person

Section 5 of the Act defines “politically exposed person” as a person who holds (or held in the past 12 months) a prominent public function in any overseas country, as well as their immediate family members. There are some significant gaps with this definition it does not cover New Zealand PEPs, persons who have been entrusted with a prominent function by an international organisation, or wider family members or close associates of PEPs.²⁸

Foreign PEPs should always be considered high risk, but domestic PEPs and PEPs from international organisations may also be high risk depending on other contextual factors. Domestic PEPs are vulnerable to being targeted by organised criminal groups or networks and susceptible to foreign interference. These risks could be mitigated by including domestic and international organisation PEPs within scope.

Requiring additional measures could complement the existing electoral finance regime, particularly if domestic PEPs included political candidates or persons who receive party donations. For example, requiring businesses to take additional measures and make further inquiries could help screen or deter payments which might breach the *Electoral Act 1993*. This could help the Electoral Commission and Serious Fraud Office appropriately respond to breaches of electoral finance rules, particularly where transactions are structured to avoid relevant disclosure requirements.

However, we would need to carefully define domestic and international organisation PEPs to ensure they align with the identified risks and ensure businesses do not have a disproportionate compliance burden. Unlike foreign PEPs, domestic PEPs and PEPs from international organisations are not always considered high risk and may only be high risk depending on other contextual factors.



- 4.81. How do you currently treat customers who are domestic PEPs or PEPs from international organisations?
- 4.82. Should the definition of ‘politically exposed persons’ be expanded to include domestic PEPs and/or PEPs from international organisations? If so, what should the definitions be?
- 4.83. If we included domestic PEPs, should we also include political candidates and persons who receive party donations to improve the integrity of our electoral financing regime?
- 4.84. What would be the cost implications of such a measure for your business or sector?

Time limitation of PEP definition


The Act prescribes strict time limits beyond which a person is no longer a PEP – i.e. if they have not held a prominent public function in the past 12 months. This is not consistent with the risk that

²⁸ The FATF defines **domestic PEPs** as individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. **International organisation PEPs** are members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

PEPs present, as a person could always remain a PEP by maintaining informal influence, even if they no longer occupy a public function. The FATF anticipates that businesses assess the risks associated with the customer to determine how to handle customers who are no longer entrusted with public functions, and not on prescribed time limits. For example, businesses should determine:

- the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or
- whether the individual’s previous and current function are linked in any way (e.g. formally by appointment of the PEP’s successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Removing the prescribed time limit in the definition of a PEP and instead using a risk-based approach would ensure that businesses continue to identify and mitigate any risks the customer presents. However, it could potentially increase compliance costs associated with those customers if businesses are not otherwise conducting enhanced CDD on former PEPs.



- 4.85. How do you currently treat customers who were once PEPs?
- 4.86. Should we require a risk-based approach to determine whether a customer who no longer occupies a public function should still nonetheless be treated as a PEP?
- 4.87. Would a risk-based approach to former PEPs impact compliance costs compared to the current prescriptive approach?

Identifying whether a customer is a PEP

Foreign PEPs


Because foreign PEPs should always be considered high risk, the FATF expects that businesses have systems and processes in place to identify whether a customer or a beneficial owner is a foreign PEP. This means that businesses should be taking *proactive steps* to determine whether a customer or beneficial owner is a foreign PEP. Importantly, the FATF does not consider simply relying on commercial databases to be sufficient.²⁹

Our law requires reporting entities to “take reasonable steps to determine whether the customer or any beneficial owner is a politically exposed person” (section 26(1)). We want to explore whether further clarity is needed regarding what is meant by this requirement, and the extent to which it aligns with the FATF’s expectations that proactive steps are taken.

In addition, we also want to explore whether businesses should be able to consider the extent to which they are vulnerable to foreign PEPs when determining the level of proactive steps that should be taken. For example, a small payday loan company may not have the same exposure to foreign PEPs as a TCSP specialising in foreign trusts: it would make more sense for the TCSP to take more proactive steps than the payday lender.

²⁹ FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22) (June 2013), footnote 6

Finally, the Act requires businesses to check whether a customer is a (foreign) PEP “as soon as practicable after establishing a business relationship or conducting an occasional transaction or activity”. This does not comply with the FATF standards, which require that businesses proactively take steps to identify whether a customer is a PEP *before* establishing a business relationship or conducting an occasional transaction or activity. The current requirements are particularly problematic for occasional transactions, as there is limited (if any) leverage for the business to retrospectively obtain the necessary information from the customer to determine whether they are a foreign PEP.




- 4.88. What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP?
- 4.89. Do you consider the Act’s use of “take reasonable steps” aligns with the FATF’s expectations that businesses have risk management systems in place to enable proactive steps to be taken to identify whether a customer or beneficial owner is a foreign PEP? If not, how can we make it clearer?
- 4.90. Should the Act clearly allow business to consider their level of exposure to foreign PEPs when determining the extent to which they need to take proactive steps?
- 4.91. Should the Act mandate that businesses undertake the necessary checks to determine whether the customer or beneficial owner is a foreign PEP *before* the relationship is established or occasional activity or transaction is conducted?

Domestic or international organisation PEPs

In contrast to foreign PEPs, the FATF allows businesses to take reasonable (rather than proactive) measures, based on the assessment of the level of risk, to determine whether the customer or beneficial owner is a domestic or international organisation PEP. This means businesses should review CDD data to determine whether the customer or beneficial owner is a domestic or international organisation PEP (or their family member or close associate).

The extent to which a business should review CDD data should depend on the risk of the business relationship: in low-risk cases, it may be appropriate for a business to not take any further steps to determine whether a customer is a PEP. As such, the FATF anticipates that businesses also gather enough information to understand the risk of the business relationship, such as by understanding the public function(s) the PEP occupies and the extent to which they have access to or control over public funds.



- 4.92. How do you currently deal with domestic PEPs or international organisation PEPs? For example, do you take risk-based measures to determine whether a customer is a domestic PEP, even though our law does not require this to be done?
- 4.93. If we include domestic PEPs and PEPs from international organisations within scope of the Act, should the Act allow for business to take reasonable steps, according to the level of risk involved, to

determine whether a customer or beneficial owner is a domestic or international organisation PEP?

- 4.94. What would the cost implications of including domestic PEPs and PEPs from international organisations be for your business or sector?

Beneficiaries of life insurance policies

The FATF requires that, in relation to life insurance policies, business should take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the pay out, and where higher risks are identified, enhanced measures should be required. Although no life insurers offer risky life insurance policies (see page 53), the lack of any requirements for determining whether a life insurance beneficiary is a PEP is a vulnerability that could be exploited.



- 4.95. Should businesses be required to take reasonable steps to determine whether the beneficiary (or beneficial owner of a beneficiary) of a life insurance policy is a PEP before any money is paid out?
- 4.96. What would be the cost implications of requiring life insurers to determine whether a beneficiary is a PEP?

Mitigating the risks of politically exposed persons

The FATF expects that businesses put in place enhanced risk mitigation measures because of the risks that PEPs present, including:

- obtaining senior management approval before establishing (or continuing) a business relationship with a PEP;
- taking reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as PEPs; and
- conduct enhanced monitoring of the relationship.

For foreign PEPs, these measures should always be applied. However, for domestic or international organisation PEPs, the FATF only requires these measures where the relationship with the PEP is considered higher risk.

Our law does not require senior management approval to establish a business relationship with a PEP (approval is only required to *continue* a business relationship). The Act also does not require enhanced monitoring of the relationship, and businesses have the option of determining source of wealth *or* source of funds (rather than wealth *and* funds). We want to explore whether the Act should explicitly require businesses to take measures consistent with the FATF's expectations. This would ensure that businesses better mitigate the risks of PEPs, but also may increase compliance costs for businesses with customers who are PEPs.



- 4.97. What steps do you currently take to mitigate the risks of customers who are PEPs?
- 4.98. Should the Act mandate businesses take the necessary mitigation steps the FATF expects for all foreign PEPs, and, if domestic or

international organisation PEPs are included within scope, where they present higher risks?

- 4.99. What would be the cost implications of requiring businesses to take further steps to mitigate the risks of customers who are PEPs?

Implementation of targeted financial sanctions

As noted above (see page 2), New Zealand implements targeted financial sanctions (TFS) against designated persons and entities through a combination of the *Terrorism Suppression Act 2002* and regulations issued under the *United Nations Act 1946*. The obligations to implement TFS are a key mechanism in the fight against terrorism and the proliferation of weapons of mass destruction. Specifically, our laws:

- require all persons to freeze, without delay, the property owned or controlled, directly or indirectly, by a designated person or entity (the ‘freezing obligation’);³⁰ and
- prohibit all persons from making property, funds, or financial or related services available to a designated person or entity unless authorised (the ‘prohibition’).³¹

All natural and legal persons (not just businesses with AML/CFT obligations) are required to implement the freezing obligation and prohibition immediately (without delay) once a person is designated by the Prime Minister or the UN. However, businesses have an important role in implementing TFS because they are more likely to be in a position of dealing the property or funds of designated persons or persons acting on their behalf.

Implementing TFS is a substantial obligation and carries potentially significant risks for business, as failure to do so is a criminal offence punishable by up to 7 years’ imprisonment or equivalent financial penalty for legal persons. Failure to implement TFS effectively also carries a risk for New Zealand, as it allows funds and services to be accessed by persons and entities known to be involved in terrorism or the proliferation of weapons of mass destruction.

Recommended Action (e) for Immediate Outcome 4 (page 100)

New Zealand should strengthen implementation of measures in relation to identification and approval of PEP relationships, and designated persons under TFS, including mandating that reporting entities screen customers’ names to ascertain PEP/sanction designation status prior to establishing business relationships.

We would like to explore whether there is more that we can do to ensure that businesses are aware of and supported in implementing their obligations under the *Terrorism Suppression Act 2002* and *United Nations Act 1946*. There are a number of potential options that we could consider. However, we are conscious that any changes to AML/CFT obligations will need to be able to be effectively implemented by all sizes and types of businesses, while also ensuring that we maintain our compliance with the UN requirements.

³⁰*Terrorism Suppression Act 2002*, s 9; *United Nations (Iran – Joint Comprehensive Plan of Action) Regulations 2016*, cl 29; *United Nations (Democratic People’s Republic of Korea) Regulations 2017*, cl 44

³¹ *Terrorism Suppression Act 2002*, s 10; *United Nations (Iran – Joint Comprehensive Plan of Action) Regulations 2016*, cl 30; *United Nations (Democratic People’s Republic of Korea) Regulations 2017*, cl 45



One key change that we could make to support effective implementation is by giving an agency or agencies the authority to supervise businesses for implementing their targeted financial sanctions obligations. This is discussed above at page 4.

Assessing exposure to designated individuals or entities and sanctions evasion

Requiring businesses to assess their potential exposure to designated individuals could be useful as a first step as it could help inform the nature of the policies, procedures, and controls a business should implement. For example, if a business identifies that it has significant exposure, it might be appropriate for that business to implement an automatic and computer-based screening solution, whereas businesses with less exposure may determine that a manual screening process is appropriate. The NRA could also be used to assess New Zealand's overall exposure to designated individuals, which would inform business-level assessments.

In addition, the FATF has updated its standards to require countries and businesses to assess their "proliferation financing risk". The FATF has defined "proliferation financing risk" as referring strictly and only to the potential breach, non-implementation, or evasion of TFS obligations. Legislation could also require businesses to assess exposure to potential proliferation financing sanctions evasion and risk in line with FATF standards or could require businesses to assess proliferation financing risks more broadly.



- 4.100. Should businesses be required to assess their exposure to designated individuals or entities?
- 4.101. What support would businesses need to conduct this assessment?
- 4.102. If we require businesses to assess their proliferation financing risks, what should the requirement look like? Should this assessment be restricted to the risk of sanctions evasion (in line with FATF standards) or more generally consider proliferation financing risks?

Including TFS implementation in an AML/CFT programme

To strengthen implementation of measures related to TFS, the Act could require businesses to include policies, procedures, and controls relating to their TFS obligations in their AML/CFT programme. Requiring the AML/CFT programme to consider implementation of TFS allows every business to determine what is appropriate and could be based on the business' assessment of their exposure to designated individuals and proliferation financing risks.

However, we would need to make it clear that businesses' policies, procedures, and controls ensure they implement TFS without delay in every circumstance. For example, the programme would need to set out how and when customer names, accounts, and transactions are screened, and how to stop attempts from designated people to open accounts or conduct transactions or activities.



- 4.103. Should legislation require businesses to include, as part of their AML/CFT programme, policies, procedures, and controls to implement TFS obligations without delay? How prescriptive should the requirement be?
- 4.104. What support would businesses need to develop such policies, procedures, and controls?

Prompt notification about designated persons and entities

Implementing TFS obligations without delay requires businesses to quickly identify designated persons and entities. As such, it is important that businesses are quickly notified once a designation has been issued or revoked, so they can identify whether a prospective (or existing customer) is a designated person or entity, and, if so, take the necessary action e.g. freezing assets or refusing to provide a service.

Currently, the government maintains a publicly available list of persons and entities subject to terrorism-related designations on the [FIU website](#) and the Ministry of Foreign Affairs and Trade website also provides links to terrorism and proliferation-related UN sanctions lists. Any changes to terrorism-related designations are notified to businesses by the FIU through goAML. However, not all businesses are registered with goAML and therefore do not receive up-to-date notifications of changes to designations. There is currently no mechanism for the government to communicate changes to proliferation-related designations to businesses.

There is no obligation on businesses to proactively keep themselves up to date with terrorism and proliferation-related designations. We could include an obligation in the Act which requires businesses ensure they are receiving updates of new or revoked designations in a timely manner. If we were to introduce this obligation, we are interested in whether businesses would want this service to be provided by the government or whether they would be comfortable relying on third-party notification services.

An additional challenge that businesses likely have is with respect to identifying people who act on behalf of or are associated with a designated person or entity, to which TFS obligations also apply. We are interested in understanding how we can better support businesses in identifying associates or people acting on behalf of designated persons or entities, which can be a significant and resource intensive task.



- 4.105. How should businesses receive timely updates to sanctions lists?
- 4.106. Do we need to amend the Act to ensure all businesses are receiving timely updates to sanctions lists? If so, what would such an obligation look like?
- 4.107. How can we support and enable businesses to identify associates and persons acting on behalf of designated persons or entities?

Screening for designated persons and entities

While government agencies can communicate designations to businesses, businesses are ultimately responsible for identifying designated customers, property or transactions. Some businesses currently use global watchlist services to automatically screen for designated persons and entities, but these services tend to be expensive and are unlikely to be appropriate for every business.

We could use the Act to better support businesses with screening for designated persons or entities. One option would be to mandate that businesses screen customer names prior to establishing a business relationship to determine whether they are a designated individual or entity. While this may reduce New Zealand's exposure to designated individuals and entities, it would impose a significant compliance cost on businesses which do not already have screening mechanisms in place. Further, although some countries with higher levels of exposure have taken this approach, ultimately it is not required by FATF standards.

Another option would be to issue a Code of Practice which sets out the steps that businesses can take to ensure they are appropriately screening customers and transactions. This would provide a legislative safe harbour under the Act and could be pursued irrespective of whether the Act mandates when screening should occur.



- 4.108. Do you currently screen for customers and transactions involving designated persons and entities? If so, what is the process that you follow?
- 4.109. How could the Act support businesses to screen customers and transactions to ensure they do not involve designated persons and entities? Are any obligations or safe harbours required?
- 4.110. If we created obligations in the Act, how could we ensure that the obligations can be implemented efficiently and that we minimise compliance costs?

Notification of actions taken

The UN and FATF require businesses to promptly notify the government of any assets frozen or actions taken in compliance with the prohibition, including whether there were any attempted transactions. This ensures that government agencies receive prompt feedback about the impact of any designation, including whether any assets were held by the designated person or entity in the country.

The *Terrorism Suppression Act 2002* requires businesses to file a "suspicious property report if they suspect on reasonable grounds that property in their possession or immediate control is property that is owned or controlled by a designated terrorist entity. There are no equivalent reporting requirements where property is frozen to comply with regulations issued under the *United Nations Act 1946*. In addition, businesses can file SARs if they have reasonable grounds for suspicion that the transaction, activity, or inquiry is relevant to the enforcement of any offence, including the offences in the *Terrorism Suppression Act 2002* and the *United Nations Act 1946*. However, the current obligations do not explicitly require businesses to report the actions they have taken.

We want to explore how we can streamline the current reporting and notification obligations, as well as ensure that there is an appropriate notification process for actions taken in compliance with regulations issued under the *United Nations Act 1946*. For example, we could create a new reporting obligation in the AML/CFT Act which complies with the UN's and FATF's requirements. If we took this step, we would ensure there is no duplication of reporting requirements in relation to the same activity.



- 4.111. How can we streamline current reporting obligations and ensure there is an appropriate notification process for property frozen in compliance with regulations issued under the *United Nations Act*?
- 4.112. If we included a new reporting obligation in the Act which complies with UN and FATF requirements, how could that obligation look? How could we ensure there is no duplication of reporting requirements?

Providing assurance for ongoing freezing action

If a business has identified property that it knows belongs or is controlled by a designated person or entity, it becomes an offence to deal with that property other than to freeze it. This effectively ensures that property owned or controlled by designated persons or entities is frozen without delay.

We want to explore whether the government should provide assurance in a timely manner to businesses who have frozen assets. For example, the Act could require any freezing actions to be reviewed (e.g. by the FIU) to provide assurance that the actions are appropriate and that assets should continue to be frozen until the person or entity is no longer designated. We could also use that process to resolve false positive matches for businesses.



- 4.113. Should the government provide assurance to businesses that have frozen assets that the actions taken are appropriate?
- 4.114. If so, what could that assurance look like and how would it work?

Correspondent banking³²

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

Correspondent banking relationships can be risky as the correspondent bank is relying on the respondent bank’s risk management. If the respondent bank is located in a higher-risk jurisdiction, or has a particularly risky customer base, the provision of banking services to that

³² New Zealand was rated largely compliant in our Mutual Evaluation for Recommendation 13, which relates to correspondent banking relationships. This rating indicates that minor deficiencies exist in our legal framework. The deficiency identified is that it is not clear correspondent banking rules apply to non-bank relationships with similar characteristics.

bank by the correspondent increases the correspondent bank’s vulnerabilities. To address these risks, the FATF requires businesses to apply additional measures in relation to the respondent business, such as assessing their AML/CFT controls and obtaining enough information to fully assess the nature of the respondent’s business and the risks they are exposed to.

Our requirements for correspondent banking relationships (in [section 29](#)) mostly comply with FATF standards but have not been substantively reviewed since they were introduced in 2013. However, one gap that was identified by the FATF is that the definition of “correspondent banking relationship” does not cover relationships outside the banking sector. Relationships which are similar to correspondent banking may exist in other sectors (e.g. global securities firms executing transactions for a cross-border intermediary), although we are not aware of any such relationships existing. If these relationships exist, they are likely exposed to similar risks and vulnerabilities to correspondent relationships in the banking sector, and it is worth considering whether the requirements in section 29 should apply.



- 4.115. Are the requirements for managing the risks of correspondent banking relationships set out in [section 29](#) still fit-for-purpose or do they need updating?
- 4.116. Are you aware of any correspondent relationships in non-banking sectors? If so, do you consider those relationships to be risky and should the requirements in [section 29](#) also apply to those correspondent relationships?

Money or value transfer service providers³³

Money or value transfer service (MVTS) providers, such as remitters, are recognised internationally and domestically as being particularly vulnerable to misuse for money laundering and terrorism financing.

MVTS can be an attractive and often lower cost option for persons that need to send money quickly to another person. Funds can also be picked up in a relatively short timeframe, as opposed to waiting for wire transfers to be processed. MVTS operators that do not operate through the formal financial system and operate ‘informal’ remittance systems are exposed to additional money laundering and terrorism financing risks.



One way that the risk of MVTS can be addressed is by requiring MVTS providers and their agents to be licensed or registered. This issue is discussed above at page 16. We also generally consider what agents can be used for above at page 40

³³ New Zealand was rated [partially compliant](#) in our Mutual Evaluation for Recommendation 14, which relates to money or value transfer services (MVTS). This rating indicates that moderate deficiencies exist in our framework, including the lack of any requirements that MVTS agents are licensed or registered. There are also no requirements for MVTS providers to maintain a list of agents which agencies can access.

Maintaining a list of agents

MVTS providers which use agents are under no obligation to maintain a list of those agents. This is inconsistent with the FATF standards and potentially increases the risks associated with using agents. The lack of a list means that DIA, as supervisor of MVTS providers, does not have visibility about how many agents are being used by MVTS providers and where those agents are located.

We could issue regulations to require MVTS providers to maintain a list of agents that they are using as part of their compliance programme. A requirement of this nature would mean that agencies, like DIA, can access this information when required. It would also ensure the MVTS provider has full visibility of how many agents it has and where they are located.

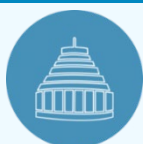
- 4.117. If you are an MVTS provider which uses agents, how do you currently maintain visibility of how many agents you have?
- 4.118. Should a MVTS provider be required to maintain a current list of its agents as part of its AML/CFT programme?
- 4.119. Should a MVTS provider be explicitly required to monitor and manage its agents for compliance with its AML/CFT programme (including vetting and training obligations)?



Ensuring agents comply with AML/CFT obligations

A related issue is that the Act does not explicitly state that a MVTS provider is responsible and liable for ensuring that all activities undertaken by an agent are compliant with its AML/CFT obligations. Under the general law of agency, the principal (i.e., the MVTS provider) is bound by the actions of their agents, but this position is not clearly stated in the Act. MVTS providers are also not required to include MVTS agents in their programmes, meaning that MVTS providers are not responsible for managing and monitoring their agents' compliance.

We can amend the Act to explicitly state that MVTS providers are liable for the compliance of their agents, which would be consistent with the general law of agency. We could further support this position by issuing regulations which require MVTS providers to include their agents in their programme, which would require them to monitor those agents and conduct vetting and training. Both of these changes would help address risks that result from using agents, but would potentially increase compliance costs for MVTS providers, particularly those who do not currently monitor their agents for compliance with AML/CFT obligations.



- 4.120. Should the Act explicitly state that a MVTS provider is responsible and liable for AML/CFT compliance of any activities undertaken by its agent? Why or why not?

- 4.121. If you are an MVTS provider which uses agents, do you currently include your agents in your programme, and monitor them for compliance (including conducting vetting and training)? Why or why not?



- 4.122. Should we issue regulations to explicitly require MVTs providers to monitor and manage its agents for compliance with its AML/CFT programme (including vetting and training obligations)? Why or why not?
- 4.123. What would be the cost implications of requiring MVTs providers to include agents in their programmes?

Multiple layers to agency relationships

The business models of some large international MVTs providers adopted in many countries is to have two layers of agents, in which a master agent is responsible for monitoring compliance of multiple sub-agents. The master agent and the sub-agents are in combination responsible for delivering the remittance service on behalf of the MVTs provider.

Our Act does not contemplate a remittance delivery model that uses two layers of agents. Where such business models have been adopted in New Zealand, it is not currently clear who is responsible and liable for AML/CFT compliance of activities undertaken by a sub-agent. Specifically, whether it the large international MVTs provider, the master agent, or both.

We are interested in understanding who should be responsible for ensuring a sub-agent complies with AML/CFT obligations. One option would be to declare the master agent to be a reporting entity and make the master agent responsible for the compliance of its sub-agents. This would be consistent with the approach taken in other countries and would ensure that responsibilities are clear where there are multiple layers to agency relationships. However, this would also have the potential to increase the compliance costs for master agents, as they would become reporting entities in their own right and have to fully comply with the AML/CFT Act.

- 4.124. Who should be responsible for the AML/CFT compliance for sub-agents for MVTs providers which use a multi-layer approach? Should it be the MVTs provider, the master agent, or both?
- 4.125. Should we issue regulations to declare that master agents are reporting entities under the Act in their own right? Why or why not?
- 4.126. What would be the cost implications of requiring MVTs providers to include agents in their programmes?



New technologies³⁴

Developing new products, business products, new delivery mechanisms, and using new or developing technologies can expose a business to emerging risks that may not have previously been considered. As a result, the FATF expects businesses identify, assess, and mitigate the risks associated with developing or using new products, practices, and technologies.

³⁴ New Zealand was rated mostly met in our Mutual Evaluation for criterion 15.1 and 15.2, which relate to the risks of new technologies. This rating indicates that minor deficiencies exist in our legal framework. The key deficiencies are that there are no explicit requirements for risk assessments of new products, business practices or technologies to be conducted prior to their launch or use, nor are mitigation measures explicitly required.

Understanding the risk of new products or technologies

The Act requires businesses to assess their business, products and delivery methods ([section 58\(2\)](#)). However, this does not explicitly require businesses to assess the risks associated with new products, business practices, delivery mechanisms and using new or developing technologies.

We want to explore whether we should issue regulations to explicitly require businesses to understand the risk of new products or technologies, e.g. requiring new technologies to be assessed when conducting a risk assessment under [section 58](#). We could also explicitly require this assessment to be conducted *prior* to the launch of a new product or similar. Alternatively, we could update existing guidance material to include these considerations (which businesses must have regard to).

- 4.127. What risks with new products or technologies have you identified in your business or sector? What do you currently do with those risks?
- 4.128. Should we issue regulations to explicitly require businesses to assess risks in relation to the development of new products, new business practices (including new delivery mechanisms), and using new or developing technologies for both new and pre-existing products? Why or why not?
- 4.129. If so, should the risks be assessed prior to the launch or use of any new products or technologies?
- 4.130. What would be the cost implications of explicitly requiring businesses to assess the risks of new products or technologies?



Mitigating the risks of new products or technologies

Businesses do not have an explicit requirement to mitigate the risks associated with new products or technologies, but do have a general obligation in [section 57\(f\)](#), and are required to mitigate the risks of products and transactions that might favour anonymity ([section 57\(i\)](#) and [section 30](#)).

We want to explore whether we should introduce an explicit requirement for businesses to mitigate any risks identified with new products or technologies, or whether the existing requirements are sufficient. If we explicitly required businesses to conduct a risk assessment of new products or technologies under section 58 that assessment would need to be factored into the obligations in [sections 30](#), [57\(f\)](#), and [57\(i\)](#).

- 4.131. Should we issue regulations to explicitly require businesses to mitigate risks identified with new products or technologies? Why or why not?
- 4.132. Would there be any cost implications of explicitly requiring business to mitigate the risks of new products or technologies?




Virtual asset service provider obligations³⁵

Recent years has seen an increase in new and innovative technologies that can be used to swiftly transfer value around the world. The fast-evolving blockchain and distributed ledger technologies have the potential to radically change the financial landscape. However, their perceived anonymity, speed, and global reach also attracts those who want to escape authorities' scrutiny. Businesses that provide services in respect of virtual assets (e.g., Bitcoin, Ethereum) have been identified internationally as being vulnerable to money laundering and terrorism financing abuse.

To combat this growing concern, the FATF updated its standards in 2019 to require countries to take action to address the risks posed by virtual asset service providers. This includes ensuring that these businesses have appropriate CDD obligations and that virtual assets transfers are treated like international wire transfers. Most types of businesses that provide virtual asset services have AML/CFT obligations (see page 27), however we have not assessed whether the existing obligations are appropriate for these businesses, whether they need to be tailored, and whether more assistance is required.

4.133. Are there any obligations we need to tailor for virtual asset service providers? Is there any further support that we should provide to assist them with complying with their obligations?




Threshold for occasional transactions

No specific threshold has been set for occasional transactions involving virtual assets. As such, the default occasional transaction thresholds apply (NZD 10,000 for cash transactions, NZD 1,000 for wire transfers). This is not in line with the significant risks that these businesses are exposed to, and lower occasional transaction thresholds have been imposed for other high-risk transactions (e.g., cash transactions in casinos and foreign currency exchange transactions). Furthermore, no CDD obligations currently apply to occasional transactions involving virtual asset to virtual asset transfers.

The FATF's expectation is that countries set an occasional transaction threshold at EUR/USD 1,000 for all transactions involving virtual assets (including virtual asset to virtual asset transfers), which would translate to approximately NZD 1,500.

4.134. Should we set specific thresholds for occasional transactions for virtual asset service providers? Why or why not?

4.135. If so, should the threshold be set at NZD 1,500 (in line with the FATF standards) or NZD 1,000 (in line with the Act's existing threshold for currency exchange and wire transfers)? Why?



³⁵ New Zealand was generally rated mostly met in our Mutual Evaluation for criteria 15.3 to 15.11, which relate to virtual asset service providers. This rating indicates that minor deficiencies exist in our legal framework. The FATF concluded that most virtual asset service providers had AML/CFT obligations, apart from some wallet providers, but no specific requirements had been introduced for CDD and wire transfers.

4.136. Are there any challenges that we would need to navigate in setting occasional transaction thresholds for virtual assets?

Declaring virtual asset transfers to be wire transfers

The FATF expects that countries treat all virtual asset transfers as cross-border wire transfers and require businesses to collect information about the people making and receiving the transfer. This is because virtual assets can enable value to be transferred globally without involving formal financial systems, which have been regulated for some time to ensure that cross-border transactions can be easily tracked and traced.

The extent to which the existing definitions of wire transfers cover transfers of virtual assets is unclear, but the definitions are unlikely to cover all types of virtual asset transfers. We can resolve this uncertainty by issuing regulations to declare these transactions as a type of wire transfers. We could also issue regulations declaring that a transfer of virtual assets is always cross-border to address the risks these types of transactions pose. This would mean that the existing identity and verification requirements for wire transfers (set out in [sections 27 to 29](#)) would apply to these transactions, as well as the requirements to file prescribed transaction reports ([section 48C](#)).

4.137. Should we issue regulations to declare that transfers of virtual assets to be cross-border wire transfers? Why or why not?

4.138. Would there be any challenges with taking this approach? How could we address those challenges?



Wire transfers³⁶

The FATF standards in relation to wire transfers have the objective of preventing terrorists and other criminals from having unregulated access to international payment systems, and to enable misuse to be easily detected. These standards are designed to ensure that basic information on the parties to the wire transfer is available to businesses and government agencies. This ensures transactions can be easily traced internationally and that suspicious activity can be identified.

Terminology involved in a wire transfer

A wire transfer is defined in [section 5](#), including when it should be considered an “international” wire transfer. Section 5 also provides definitions of the institutions involved in wire transfers (ordering, intermediary, and beneficiary institutions). However, we have identified a number of challenges with the definitions used, such as:

- **the definition of a wire transfer excludes credit and debit card transactions** if the credit or debit card number accompanies the transaction. As a result, some international

³⁶ New Zealand was rated [partially compliant](#) in our Mutual Evaluation for Recommendation 16, which relates to wire transfers. This rating indicates that moderate deficiencies exist in our legal framework. Key deficiencies include there being no requirements for wire transfers less than NZD, no requirements for full beneficiary information to be maintained, and there is no prohibition on executing wire transfers where the rules cannot be complied with.

transfers of funds (e.g. original credit transactions) are not subject to the same scrutiny or reporting obligations. This is also partially inconsistent with the FATF standards.³⁷

- the definition of wire transfer does not reflect the **technical, legal, and practical realities of the ways that banks and non-bank businesses interact with each other**. In particular, it does not reflect how SWIFT messaging operates, including where businesses are transferring funds on behalf of its underlying client through banks.
- the definition of wire transfer **only uses the phrase “reporting entity”**. It is unclear how these provisions apply to international wire transfers that involve businesses outside of New Zealand as those businesses might not meet our definition of a reporting entity.
- an international wire transfer needs to have **one of the institutions involved “outside” New Zealand**. Determining whether a business is “outside” New Zealand can be challenging where businesses have offices in New Zealand but bank accounts in other countries which are used partially or fully to carry out the wire transfer.



- 4.139. What challenges have you encountered with the definitions involved in a wire transfer, including international wire transfers?
- 4.140. Do the definitions need to be modernised and amended to be better reflect business practices? If so, how?
- 4.141. Are there any other issues with the definitions that we have not identified?

Ordering institutions

The ordering institution is the businesses which has been instructed by a person (the payer or originator) to transfer funds to another person (the payee or beneficiary). [Sections 27](#) and [28](#) set out that wire transfers of NZD 1000 or above must be accompanied by specific information about the originator to enable the transaction to be traced back to that person if needed.

Wire transfers below the applicable threshold

There are no requirements to ensure that international wire transfers of less than NZD 1000 are accompanied by some information about the originator and beneficiary. In particular, there is no requirement that these wire transfers are always accompanied by the following:

- the name of the originator and their account number or unique transaction reference number which permits traceability of the transaction;
- the name of the beneficiary and their account number or unique transaction reference which permits traceability of the transaction.

The information that should be collected and provided for wire transfers below the threshold is less than what is required for wire transfers above NZD 1000, and we understand that some

³⁷ The FATF notes that the wire transfer requirements in Recommendation 16 are not intended to cover any transfer that flows from a transaction carried out using credit or debit or prepaid card for the purchasing of goods or services, so long as the card number accompanies all transfers flowing from the transaction. However, where the card is used as a payment system to affect a person-to-person wire transfer, the transaction is covered by Recommendation 16 and the necessary information should be included in the message.


businesses, particularly banks, already provide this information despite there being no obligation to do so. However, the lack of any requirements is inconsistent with the FATF standards and presents a vulnerability that undermines the traceability of transactions. Some high-risk transactions (e.g. terrorism financing, child exploitation payments) are commonly below NZD 1000.

We can issue regulations to require that international wire transfers below NZD 1000 are accompanied with specific information about the originator and beneficiary. The information would not need to be verified for accuracy unless there is a suspicion of money laundering or terrorism financing. This would address the vulnerability we have identified and improve compliance with the FATF standards. However, it may also increase compliance costs, particularly for businesses which regularly conduct international wire transfers below NZD 1000 and who are not already collecting and providing the required information.

4.142. What information, if any, do you currently provide when conducting wire transfers below NZD 1000?

4.143. Should we issue regulations requiring wire transfers below NZD 1000 to be accompanied with some information about the originator and beneficiary? Why or why not?


4.144. What would be the cost implications from requiring specific information be collected for and accompany wire transfers of less than NZD 1000?



Stopping wire transfers that lack the required information

The FATF standards require ordering institutions to be prevented from executing wire transfers where information is missing. In practice, [section 37](#) prohibits wire transfers from being conducted where there is missing information about the originator. However, there is no explicit requirement to stop executing a wire transfer where it lacks the required beneficiary information (i.e. name and account number), and the existing prohibitions do not apply to wire transfers below NZD 1000.

We want to explore whether we should explicitly prohibit ordering institutions from executing wire transfers that do not have the required information about the originator and beneficiary. This would guarantee that ordering institutions are provide the beneficiary’s name and account number with the wire transfer, which would ensure that the beneficiary institution pays money to the correct person. We do not anticipate that an explicit prohibition would significantly impact compliance costs for most ordering institutions, as it would be impossible to initiate a wire transfer without at least some information about the beneficiary.



4.145. How do you currently treat wire transfers which lack the required information about the originator or beneficiary, including below the NZD 1000 threshold?

4.146. Should ordering institutions be explicitly prohibited from executing wire transfers in all circumstances where information about the parties is missing, including information about the beneficiary? Why or why not?

4.147. Would there be any impact on compliance costs if an explicit prohibition existed for ordering institutions?

Intermediary institutions

The intermediary institution is the business which receives and transmits the wire transfer on behalf of the ordering and beneficiary institutions. There may be one or more intermediary institution involved in an international wire transfer, depending on the destination country and the other businesses involved.

The main obligation on intermediary institutions is to pass the wire transfer along the chain, including the information about the originator and beneficiary. Our Act does not mandate that the information be retained with the wire transfer, but just that the information be provided as soon as practicable ([section 27\(6\)](#)). This is not in line with the FATF standards and risks transfers being delayed or information being lost about the originator and beneficiary.



4.148. When acting as an intermediary institution, what do you currently do with information about the originator and beneficiary?

4.149. Should we amend the Act to mandate intermediary institutions to *retain* the information with the wire transfer? Why or why not?

In addition, the FATF requires intermediary institutions to:

- keep a record, for at least five years, of all information received from the ordering or another intermediary institution where technical limitations prevent the required originator information or beneficiary from remaining with a related domestic wire transfer;
- take reasonable measures, which are consistent with straight-through processing, to identify international wire transfers which lack the required originator or beneficiary information; and
- have risk-based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking the required information, and (b) the appropriate follow-up action.

The Act does not currently require intermediary institutions to take any of the steps the FATF requires, however we understand that some intermediary institutions take these steps voluntarily. The lack of any requirements means that intermediary institutions are a potential vulnerability for international payments and may not be picking up on and dealing with wire transfers that lack the required information. In addition, intermediary institutions which self-impose these obligations may be at a competitive disadvantage compared with other intermediaries which do not.

We can issue regulations which would require intermediary financial institutions to keep the relevant records and have relevant measures, policies and procedures in place. This would address the identified vulnerabilities and ensure that all intermediary institutions have the same compliance obligations. However, this would also potentially increase the compliance obligations for intermediary institutions, particularly those which do not already have relevant measures, policies and procedures in place.

4.150. If you act as an intermediary institution, do you do some or all of the following:



- keep records where relevant information cannot be passed along in the domestic leg of a wire transfer where technical limitations prevent the information from being accompanied?
- take reasonable measures to identify international wire transfers lacking the required information?
- have risk-based policies in place for determining what to do with wire transfers lacking the required information?

4.151. Should we issue regulations requiring intermediary institutions to take these steps, in line with the FATF standards? Why or why not?

4.152. What would be the cost implications from requiring intermediary institutions to take these steps?

Beneficiary institutions

The beneficiary institution is the business at the end of the wire transfer who makes the money available to the payee or beneficiary. The FATF standards require beneficiary institutions to take reasonable steps to identify wire transfers lacking the required information, verify the identity of the beneficiary for wire transfers above the applicable threshold, and have risk-based policies in place for how to handle wire transfers which lack the required information.

Our Act is mostly in line with the FATF standards. However, it lacks any explicit requirements for beneficiary institutions take reasonable measures, which may include post-event or real time monitoring, to identify international wire transfers that lack the required information. This may mean that some beneficiary institutions are completing wire transfers that do not have the required information about the parties. We could issue regulations to address this small vulnerability and bring New Zealand more in line with FATF standards. However, doing this may increase compliance costs for beneficiary institutions which do not currently take reasonable measures to identify wire transfers that lack required information.

4.153. Do you currently take any reasonable measures to identify international wire transfers that lack required information? If so, what are those measures and why do you take them?

4.154. Should we issue regulations requiring beneficiary institutions to take reasonable measures, which may include post-event or real time monitoring, to identify international wire transfers that lack the required originator or beneficiary information?


4.155. What would be the cost implications from requiring beneficiary institutions to take these steps?



Prescribed transaction reports

Prescribed transaction reporting (PTR) obligations were introduced in 2015 to enable the collection of financial intelligence on flows of money and value into, out of, and around New Zealand. PTRs also provide the FIU with an overview of how transactions are occurring across the economy, including risky transactions. While the FATF does not require countries to mandate

the collection of transaction information above a certain threshold, an increasing number of countries require businesses to make these types of reports.



4.156. Are the prescribed transaction reporting requirements clear, fit-for-purpose, and relevant? If not, what improvements or changes do we need to make?

4.157. Have you encountered any challenges in complying with your PTR obligations? What are those challenges and how could we resolve them?


Types of transactions requiring reporting

Only two types of transactions are declared as “prescribed transactions”: international wire transfers and domestic physical cash transactions. However, it is not always clear in every instance whether a transaction is an international wire transfer or a domestic physical cash transaction. For example, some currency exchange transactions may be treated as a cash deposit and withdrawal or international wire transfers, depending on how the business actually changes currency from one type to another. In addition, some transactions are excluded from the scope of prescribed transaction (such as credit card transactions) because of how a wire transfer is defined.

To avoid unnecessary compliance costs, businesses should have clear requirements about what transactions need to be reported as a PTR. Clear PTR obligations also ensure that the FIU receives valuable financial intelligence in all necessary instances. We could issue regulations or a Code of Practice to identify the common types of transactions where obligations are unclear and clarify whether and in what circumstances a PTR is required. This approach could also identify who is required to report in each transaction, and what information is required.

4.158. Should we issue regulations or a Code of Practice to provide more clarity about the sorts of transactions that require a PTR?

4.159. If so, what transactions have you identified where the PTR obligation is unclear? What makes the reporting obligation unclear, and how could we clarify the obligation?



Who is required to submit a report

Non-bank financial institutions and DNFBPs

It is currently unclear whether DNFBPs or non-bank financial institutions are required to file a PTR when they transfer or receive funds internationally (for example into or out of their trust account) via the banking system on behalf of an underlying customer. One view is that it is the bank, not the DNFBP or non-bank financial institution, that is engaging in the transaction and therefore has the PTR obligations. However, the bank does not have visibility of the underlying customer, and a PTR submitted by a non-bank financial institution or DNFBP would be more valuable as it would include this information.

We would like to explore options for addressing this issue and ensuring that valuable intelligence is provided while also ensuring businesses have clear obligations. One option is to require a bank that is transferring funds internationally on behalf of a DNFBP or other non-bank financial institution to submit a PTR that contains details of the underlying customer. However, noting that banks have automated PTR systems, this option may be challenging to implement for banks as it may require banks to separate out and implement additional steps for certain customers. Further steps may also be required to determine whether the businesses are transferring funds on their own behalf or on behalf of an underlying customer.

Another option is to have different reporting requirements for banks and non-bank financial institutions or DNFBPs involved in an international wire transfer, and that each party reports the information it holds. This option would enable banks to implement automated solutions and there would be no requirement to differentiate between different types of customer and transactions. The non-bank financial institution or DNFBP would then provide information about their customer to the FIU. We could also require specific transaction reference identifiers to be reported to enable the FIU the non-bank financial institution or DNFBP's PTR with the bank's PTR.

4.160. Should non-bank financial institutions (other than MVTs providers) and DNFBPs be required to report PTRs for international fund transfers?

4.161. If so, should the PTR obligations on non-bank financial institutions and DNFBPs be separate to those imposed on banks and MVTs providers?

4.162. Are there any other options to ensure that New Zealand has a robust PTR obligation that maximises financial intelligence available to the FIU, while minimising the accompanying compliance burden across all reporting entities?



Intermediary institutions

Intermediary institutions are currently exempt from making prescribed transaction reports under section 48A.

However, due to the complex ways that MVTs providers undertake wire transfers, particularly informal MVTs providers, there may be unintended gaps in PTR obligations resulting in the FIU missing important intelligence about cross border financial flows. For example, PTRs may not be submitted where multiple MVTs providers are involved in the transfer of funds as a result of the current exemption. Banks also may not realise that a payment into a customer's bank account from an MVTs provider is an incoming international wire transfer and, as a result, not submit a PTR.

One potential solution is to amend the existing regulatory exemption so that it does not apply to MVTs providers. This would ensure all wire transfer transactions, and parties to them, are properly reported to the FIU and would not impact the status quo position for banks or other businesses involved in international wire transfers.

- 4.163. Should we amend the existing regulatory exemption for intermediary institutions so that it does not apply to MVTs providers?
- 4.164. Are there any alternative options that we should consider which ensure that financial intelligence on international wire transfers is collected when multiple MVTs providers are involved in the transaction?
- 4.165. Are there any other intermediary institutions that should be included in the exemption?



When reports must be made

Section 48A requires PTRs to be made “as soon as practicable, but not later than 10 working days after the transaction occurs.” While this may be a reasonable timeframe in many circumstances, there may be situations where the timeframe is impossible to comply with. One example may be where a business does not have all the necessary information to submit a PTR and needs to request the information from other businesses involved in the transaction. Another example could be where a technological solution does not correctly identify transactions requiring PTRs, resulting in some PTRs not being reported. We want to explore whether the timeframe for submitting PTRs is still fit-for-purpose or whether there are changes we should make to the timeframe.



- 4.166. Are there situations you have encountered where submitting a PTR within the required 10 working days has been challenging? What was the cause of that situation and what would have been an appropriate timeframe?

Applicable threshold for reporting prescribed transactions

Prescribed transaction reports are required for domestic cash transactions which exceed NZD 10,000 and international wire transfers which exceed NZD 1,000. However, we would like to explore whether a lower threshold is more appropriate for New Zealand’s risk environment, particularly given the increased threat that terrorism financing presents to the safety of New Zealand.

In particular, we would like to explore whether it may be more appropriate to remove the threshold for international wire transfers, considering our risk environment and relationships with international partners. There have been a number of suspected terrorism financing and child exploitation payments moved through New Zealand, which typically fell under the NZD 1,000 threshold. Removing the threshold would require all international wire transfers to be reported.

Similarly, a lower cash transaction reporting threshold may be more appropriate, particularly as it applies to the high value dealer sector. There has been a low number of prescribed transaction reports submitted by high value dealers. This could indicate transactions are being structured to avoid the reporting threshold.



A related issue is whether the threshold for high value dealer obligations is set at the right amount. This is discussed above (see page 24).

We are aware that there are a large number of practical issues that businesses have faced in trying to comply with their obligations to file PTRs. While a lower threshold may be more appropriate, we would not look to change the threshold without first addressing the practical issues with these reports.



- 4.167. Do you consider that a lower threshold for PTRs to be more in line with New Zealand's risk and context? If so, what would be the appropriate threshold for reporting?
- 4.168. Are there any practical issues not identified in this document that we should address before changing any PTR threshold?
- 4.169. How much would a change in reporting threshold impact your business?
- 4.170. How much time would you need to implement the change?

Reliance on third parties³⁸

Relying on a third party to conduct CDD is one of the main ways that businesses can reduce their compliance obligations, particularly where a customer is in another country or where there are multiple businesses involved in a transaction or activity. However, reliance is not without its risks or vulnerabilities: there is a greater distance between the business and the customer, the relied upon party may have a different idea of what is considered “risky”, and they may not identify suspicious indicators or red flags. As such, our Act imposes a number of restrictions as to when a third party can be relied upon for AML/CFT purposes.

Effectiveness of reliance provisions

Our Act allows reporting entities to rely on third parties in three circumstances:

1. relying on a member of a DBG ([section 32](#))
2. relying on another reporting entity in New Zealand or a person in another country that has sufficient AML/CFT systems and measures in place and who is regulated for AML/CFT purposes ([section 33](#)) and has agreed to be relied upon;
3. relying on an agent ([section 34](#)).

³⁸ New Zealand was rated largely compliant in our Mutual Evaluation for Recommendation 17, which relates to reliance on third parties. This rating indicates minor deficiencies exist in our legal framework. The main deficiencies identified relate to the ability for reporting entities to rely on non-reporting entities in certain designated business groups, as well as having insufficient requirements for reporting entities to have regard to the level of country risk for overseas based third parties.

Businesses can share their compliance obligations to differing extents depending on the type of reliance employed. For example, businesses outside of a DBG can only rely on other reporting entities or persons in other countries for CDD purposes, whereas DBG members can also rely on other DBG members to make SARs or conduct risk assessments.



- 4.171. Do you use any of the reliance provisions in the AML/CFT Act? If so, which provisions do you use?
- 4.172. Are there any barriers to you using reliance to the extent you would like to?
- 4.173. Are there any changes that could be made to the reliance provisions that would mean you used them more? If so, what?

“Approved entities” and liability for reliance

When relying on a third party or a DBG member, the relying party is still responsible for ensuring that the Act is complied with. This requirement is in line with the FATF standards and ensures that businesses are not making themselves more vulnerable to money laundering or terrorism financing by relying on another business for their compliance obligations.

One exception to this is section 33(3A), which means that a business is not responsible for ensuring CDD is carried out in accordance with the Act if, among other things, the third party is an “approved entity”. This option was introduced when the Act was amended in 2017, with the intention that the government would then identify particular entities that were complying with the Act that other businesses can rely on. However, this approach is not consistent with FATF standards, and as no entities have been approved, cannot be used in practice.



- 4.174. Given the “approved entities” approach is inconsistent with FATF standards and no entities have been approved, should we continue to have an “approved entities” approach?
- 4.175. If so, how should the government approve an entity for third party reliance? What standards should an entity be required to meet to become approved?
- 4.176. If your business is a reporting entity, would you want to be an approved entity? Why or why not?
- 4.177. Are there any alternative approaches we should consider to enable liability to be shared during reliance?


Designated business group reliance


Forming a DBG allows for a broad range of reliance to occur. However, businesses must meet the eligibility criteria set out in section 5(1) of the Act to form a DBG which may inadvertently exclude some business relationships from being able to form a DBG and thereby share compliance obligations. We can issue regulations to prescribe other types of businesses that are eligible to form a DBG, and we are interested in understanding whether we need to change the existing eligibility criteria.

One small gap in our DBG reliance settings is that there is no obligation on overseas DBG members to conduct CDD to the level required by our Act. While overseas DBG members need to be located in countries with sufficient AML/CFT systems, this is not the same as ensuring that the CDD being conducted meets the requirements of our Act. This is a potential vulnerability as it could mean that insufficient CDD is being conducted by overseas DBG members despite being in a country with “sufficient” AML/CFT systems.

4.178. Should we issue regulations to enable other types of businesses to form DBGs, if so, what are those types of businesses and why should they be eligible to form a DBG?

4.179. Should we issue regulations to prescribe that overseas DBG members must conduct CDD to the level required by our Act?





4.180. Do we need to change existing eligibility criteria for forming DBGs? Why?

4.181. Are there any other obligations that DBG members should be able to share?

Third party reliance

There are some small gaps in our provisions which enable businesses to rely on third parties for CDD purposes, including third parties in other countries. In particular, there are no explicit requirements for businesses to:


- consider the level of country risk when determining whether a third party in another country can be relied upon;
- take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and
- be satisfied that the third party has record keeping arrangements in place.

These gaps may increase money laundering and terrorism financing vulnerabilities for third party reliance. It would be inappropriate for businesses to rely on other parties in high-risk jurisdictions. It is also important that copies of identification data or documents can be made available without delay, given these documents may be needed to file a SAR or can be requested by an AML/CFT supervisor. Ensuring that the third party has appropriate record-keeping arrangements in place will make it easier for the third party to provide appropriate documents without delay, if needed. However, explicitly requiring these conditions be fulfilled may present a temporary barrier to third party reliance and increase compliance costs.

We can address these gaps through issuing regulations. We are also interested in understanding whether there are any other issues with third party reliance or improvements that we can make.

4.182. Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD:

- consider the level of country risk when determining whether a third party in another country can be relied upon;



- take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and
- be satisfied that the third party has record keeping arrangements in place.

4.183. Would doing so have an impact on compliance costs for your business? If so, what is the nature of that impact?



4.184. Are there any other issues or improvements that we can make to third party reliance provisions?

Potential other forms of reliance

We are also interested in understanding whether the Act should allow for other forms of reliance to occur to help reduce unnecessary duplication of compliance obligations, especially where multiple businesses are involved in the same transaction or activity. However, any new reliance provisions would need to be tightly constrained to ensure we do not increase money laundering and terrorism financing vulnerabilities.



4.185. Are there other forms of reliance that we should enable? If so, how would those reliance relationships work?

4.186. What conditions should be imposed to ensure we do not inadvertently increase money laundering and terrorism financing vulnerabilities by allowing for other forms of reliance?

Internal policies, procedures, and controls³⁹

Internal policies, procedures, and controls are what businesses are required to implement to protect themselves against the money laundering and terrorism financing risks to which they are exposed. This includes developing and regularly reviewing its compliance programme and appointing a compliance officer.

Compliance programme requirements

Section 57 sets out the minimum requirements for a business' compliance programme. This includes requiring that there are adequate policies, procedures and controls in place for vetting

³⁹ New Zealand was rated partially compliant in our Mutual Evaluation with Recommendation 18, which relates to internal controls and foreign branches and subsidiaries. This rating indicates that moderate deficiencies exist in our legal framework. The main deficiencies identified are that there is no requirement for compliance officers to be appointed at the management level, or for financial groups to implement group-wide programmes against money laundering and terrorism financing.

and training staff, and complying with CDD, account monitoring, record keeping, and reporting obligations.



4.187. Are the minimum requirements set out still appropriate? Are there other requirements that should be prescribed, or requirements that should be clarified?

Compliance officers

Compliance officers play a key role in the administration and maintenance of a business' AML/CFT programme. The Act requires an employee to be designated as a compliance officer, or if no employees are available, the business can appoint another person.

While the Act requires that the compliance officer must report to a senior manager, this is not consistent with international standards and best practice. For example, the FATF requires compliance officers to be "at the management level". This is best practice because it puts the compliance officer in a position where they can influence higher-level decisions within the business and ensures that senior management is involved in the business' AML/CFT programme.

A separate issue is that some businesses have appointed legal persons as compliance officers, such as companies, if they have no employees who can fulfil this role. This is not the intention of the Act, and it is important that the compliance officer is a natural, rather than legal, person, so that they can act as a point of contact and drive compliance culture within the business.



- 4.188. Should the Act mandate that compliance officers need to be at the senior management level of the business, in line with the FATF standards?
- 4.189. Should the Act clarify that compliance officers must be natural persons, to avoid legal persons being appointed as compliance officers?

Group-wide programme requirements

The FATF anticipates that groups of financial or non-financial businesses⁴⁰ implement group-wide programmes against money laundering and terrorism financing. This programme should apply to all branches and majority-owned subsidiaries of the group, e.g., multi-national companies with branches in multiple countries. The group-wide programme should require what is normally required by a compliance programme, but also set out policies and procedures for information sharing within the group, how group-level compliance, audit, and/or AML/CFT functions should be provided (e.g. group-level transaction monitoring), and adequate safeguards to ensure confidentiality of information exchanged.

The AML/CFT Act currently has no specific requirements requiring financial and non-financial groups to implement group-wide programmes. The Act allows members of DBGs to share

⁴⁰ The FATF's defines financial groups as "a group that consists of a parent company or of any other type of legal persons exercising control and coordinating functions over the rest of the group for the application of group supervision under Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

compliance programmes (section 32(1)(b)) but financial and non-financial groups are not required to form DBGs. The Act also requires business to ensure that branches and subsidiaries in other countries comply with measures “broadly equivalent to those set out in this Act” (section 61(1)), but this is also not the same as mandating group-wide programmes.

Businesses operating in groups are exposed to particular risks that a group-wide programme could mitigate. In particular:

- businesses within a group may introduce customers to other parts of the group, and there may be assumptions that the customer has already been subject to sufficient CDD, which may not be the case;
- there can be inconsistencies or gaps in risk understanding and mitigation across the group, such as different group members coming to different conclusions about customer risk, due either to different risk appetites or risk information being available;
- it can be difficult to see a customer’s footprint across a group which limits the group member’s ability to accurately assess risks and can allow for criminals to make use of regulatory arbitrage between members of the group; and
- the group may undertake more than one type of activity within and across more than one jurisdiction, but all activities should be identified, assessed, and mitigated consistently and appropriately across the group.

Finally, while not a money laundering or terrorism financing risk, there may be reputational damage if risks arise as a result of poor group-wide policies and procedures or deliberate regulatory arbitrage. In other words, poor compliance from a member within a group impacts the reputation of the group overall.



4.190. If you are a member of a financial or non-financial group, do you already implement a group-wide programme even though it is not required?

4.191. Should we mandate that groups of financial and non-financial businesses implement group-wide programmes to address the risks groups are exposed to?

Review and audit requirements

It is important that business’ compliance programmes are kept up-to-date and reflect the business’ current risks, given the money laundering and terrorism financing risk environment is dynamic and changes regularly. To that end, the Act requires businesses to review their risk assessments and AML/CFT programme and ensure it is “up to date” (section 59(1)(a)). However, there is no timeframe specified for how often businesses should be conducting internal reviews and no definition of what “up to date” means.

Businesses are also required to have their programme independently audited every three years (sections 59(2) and 59B(1)). However, the Act does not state what the purpose of the audit is, which means the scope and desired outcomes are unclear. The FATF states that the purpose of the independent audit function is to “test the system” and some countries (e.g. Canada, United States, United Kingdom) explicitly state that the purpose of the audit function is to test whether the system is effective at detecting money laundering or terrorism financing.

We are also aware that there are some practical issues with the requirement for an independent audit, such as audits being expensive, of variable quality, and there may be a shortage of suitably qualified persons to conduct an audit. There is also uncertainty about the level of assurance expected from an independent audit, what actions should follow once an audit has been conducted, and how the provisions regarding legal professional privilege impact audits. We are interested in understanding how to make the audit function work better for businesses.



- 4.192. Do we need to clarify expectations regarding reviewing and keeping AML/CFT programmes up to date? If so, how should we clarify what is required?
- 4.193. Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system?
- 4.194. What other improvements or changes could we make to the independent audit or review requirements to ensure the obligation is useful for businesses without imposing unnecessary compliance costs?

Higher-risk countries⁴¹

The AML/CFT Act requires, in various places, businesses to understand the risks of the countries they deal with. In some situations, a customer being based in a particular country will elevate the risk of that customer and require additional measures to be taken. In other situations, businesses cannot rely reporting entities in countries with insufficient AML/CFT controls for CDD. Finally, some countries are so risky that the FATF has drawn attention to them, including asking countries to mandate that reporting entities apply additional measures to business relationships and transactions with persons from the country to counter the global risks they pose.

Understanding country risk and identifying countries with insufficient AML/CFT measures in place

The Act requires businesses to have regard to the countries they deal with as part of their risk assessment and include measures in their programmes to mitigate any risks associated with those countries. In addition, the Act imposes a mandatory enhanced CDD requirement on customers from a country that has “insufficient AML/CFT systems or measures” in place. However, having insufficient AML/CFT systems or measures is not the same as being high risk, nor should countries with “sufficient” AML/CFT systems never be considered risky.

The supervisors have issued guidance to businesses to help them understand how a country can impact their risk profile. Nonetheless, determining country risk can be challenging. This is particularly true for smaller businesses which may not have the resources to put towards

⁴¹ New Zealand was rated partially compliant in our Mutual Evaluation for Recommendation 19, which relates to higher-risk countries. This rating indicates that moderate deficiencies exist in our legal framework. The main deficiencies identified relate to the range of enhanced CDD measures, as well as having insufficient requirements for reporting entities to apply enhanced CDD, proportionate to the risks, to customers and transactions involving countries for which this is called for by the FATF.

assessing whether a customer from a specific country should be considered higher risk due to their location.

In addition, the FATF publicly identifies certain countries that have been assessed as having strategic deficiencies in their AML/CFT regimes and are actively working to address them under increased monitoring (sometimes known as the “grey list”).⁴² However, not every country that has strategic deficiencies is on that list: only countries that have large enough economies get publicly identified by the FATF. Countries with small economies and weak AML/CFT systems are not on that list, but nonetheless may be considered high risk.



4.195. How can we better enable businesses to understand and mitigate the risk of the countries they deal with, and determine whether countries have sufficient or insufficient AML/CFT systems and measures in place? For example, would a code of practice (rather than guidance) setting out the steps that businesses should take when considering country risk be useful?

Imposing countermeasures where called for by the FATF

Where countries are both high-risk and non-cooperative with efforts by the FATF to improve their systems, the FATF can call for countries to apply enhanced CDD and countermeasures to mitigate the global risks these countries pose. This list of countries subject to a ‘Call to Action’ (sometimes known as the “blacklist”)⁴³ currently has two countries on it: Democratic People’s Republic of Korea and Iran.

Section 22 the Act requires businesses to consider country risk and mitigate those risks, including applying enhanced CDD to non-resident customers from countries with insufficient AML/CFT systems. However, this does not meet FATF requirements because it does not apply broadly to business relationships and transactions with persons from FATF blacklisted countries. However, we can issue regulations under section 155 to prohibit or regulate business relationships and transactions with persons in particular countries. We could use this power to require effective and proportionate countermeasures against countries on the blacklist, such as limiting or prohibiting business relationships with persons in these countries, requiring enhanced CDD, or requiring systematic reporting of transactions with these countries.

- 4.196. Should we issue regulations to impose proportionate and appropriate countermeasures to mitigate the risk of countries on FATF’s blacklist?
- 4.197. If so, what do you think would be appropriate measures to counter the risks these countries pose?
- 4.198. Is the FATF blacklist an appropriate threshold? If not, what threshold would you prefer?



⁴² <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2021.html>

⁴³ <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html>

Imposing sanctions on specific individuals or entities

Section 155 allows regulations to be issued which prohibit transactions and business relationships between reporting entities. These regulations can be of general application or can apply to specific parties or countries.

New Zealand is seen as an attractive place to do business and enjoys a strong international reputation for low corruption and high levels of integrity. As such, individuals involved in significant criminality, including corruption, may see New Zealand as an attractive destination country for their illicit wealth. We could use the regulation making power in section 155 to prohibit business relationships or transactions with such individuals and, in doing so, further protect New Zealand from the money laundering risks such individuals present.

However, if we took this step, we would need to carefully consider what amendments are needed to ensure the power is used appropriately. For example, we would need to consider on what basis decisions of this nature can be made and what amount of evidence the Governor-General needs in order to impose a countermeasure against an individual. We would also need to consider how the rights of bona fide third parties are protected when countermeasures are imposed, as well as whether there should be any process for affected parties to apply to revoke a countermeasure once made.



- 4.199. Should we use section 155 to impose countermeasures against specific individuals and entities where it is necessary to protect New Zealand from specific money laundering threats?
- 4.200. If so, how can we ensure the power is only used when it is appropriate? What evidence would be required for the Governor-General to decide to impose a countermeasure?
- 4.201. How can we protect the rights of bona fide third parties?
- 4.202. Should there be a process for affected parties to apply to revoke a countermeasure once made? If so, what could that process look like?

Suspicious activity reporting

Improving the quality of reports received

On average, New Zealand businesses submitted approximately 10,500 SARs per year between 2016 and 2019,⁴⁴ with banks submitting over half of these reports. However, the FIU sometimes receives SARs with limited or no useful intelligence. This may be a result of “defensive reporting” or uncertainty as to what constitutes suspicion, what the threshold is, and when the three day is timeframe is triggered. These challenges are further compounded by the fact that businesses face substantial penalties for failing to report a suspicious activity, and some businesses may be unable to properly report due to legal privilege. In addition, there is no obligation or ability to update a SAR when additional information is obtained.

⁴⁴ Mutual Evaluation Report of New Zealand, Table 3.2.

In general, a smaller number of higher quality SARs would provide better intelligence. We therefore want to understand how we can modify the obligation to ensure this happens.



- 4.203. How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?
- 4.204. What barriers might you have to providing high quality reporting to the FIU?
- 4.205. Should the threshold for reporting be amended to not capture low level offending?

Sharing SARs or SAR information

The Act strictly limits the circumstances in which people can share information about SARs or SARs themselves ([section 46](#)). For example, businesses cannot disclose SAR information to anyone other than specific types of persons, and only Police employees can share information with other agencies or the public, provided it is shared for law enforcement purposes. This helps ensure that knowledge about suspicion is tightly controlled and that the subject of the suspicion is not inadvertently notified or ‘tipped off’.

However, there are potentially other circumstances in which sharing SARs or SAR information could be beneficial. For example:

- **allowing Police employees to share SAR information for specified non-law enforcement purposes**, such as for tax administration purposes, or providing information about bankrupt companies going through insolvencies;
- **allowing businesses to disclose to offshore parent companies** where there is no DBG formed, to enable the parent company to be aware of the risks the subsidiary is exposed to.

It may also be beneficial for businesses to share information with other businesses before submitting a SAR. This could be done to enable the origin of the suspicious funds to be properly identified and could improve the quality of the SAR received. It could also enable businesses to work together to help produce a detailed SAR. For example, US legislation enables businesses to make an application to FinCEN (the United States’ FIU) to share information with other businesses.



- 4.206. Should we expand the circumstances in which SARs or SAR information can be shared? If so, in what circumstances should this information be able to be shared?
- 4.207. Should there be specific conditions that need to be fulfilled before this information can be shared? If so, what conditions should be imposed (e.g. application to the FIU)?

SAR obligations for MVTs providers

We want to explore whether we should issue regulations that require MVTs providers to consider both sides of a transaction to determine whether a SAR should be filed. Because MVTs providers can be involved in both sides of the transaction, they may be in a position to spot suspicious activity that otherwise might not be spotted. The FATF recommends MVTs providers which control both the ordering and beneficiary end of a wire transfer should consider information from both sides of the transfer to determine whether a SAR is required. If a SAR is required, this should be submitted to the FIU in any of the countries affected by the suspicious transfer.

- 4.208. Should we issue regulations to state that a MVTs provider that controls both the ordering and beneficiary ends of a wire transfer is required to consider both sides of the transfer to determine whether a SAR is required? Why or why not?
- 4.209. If a SAR is required, should it be explicitly stated that it must be submitted in any jurisdiction where it is relevant?



High value dealer obligations

Dealers in high value goods have fewer AML/CFT obligations in comparison to other types of businesses covered by the Act. For example, high value dealers are not required to undertake risk assessments or implement an AML/CFT programme, nor are they under a mandatory obligation to submit SARs.

In part, the rationale for lessened obligations was due to the broad and diverse nature of the sector, as well the fact that most dealers in high value items were not otherwise subject to complex regulation. However, we have subsequently identified some challenges with this approach. For example, high value dealers may not fully understand their money laundering and terrorism financing risks as they are not required to conduct a risk assessment and may not be reporting suspicious activities because they are not obliged to do so.

In addition, the limited obligations pose challenges for DIA as supervisor. DIA cannot check whether high value dealers understand their money laundering and terrorism financing risks without a risk assessment or programme to review. Instead, DIA can only focus on whether CDD has been conducted in the appropriate circumstances.

We would like to explore whether high value dealers should be subject to the same obligations as other businesses. Some of these obligations (e.g., CDD) would only arise when a high value dealer engages in a cash transaction (or series of related cash transactions) above the relevant threshold, which is currently NZD 10,000. These obligations would be:⁴⁵

- full customer due diligence obligations, including enhanced CDD;*
- keeping records of transactions;
- identifying and managing the risks of any politically exposed persons;*
- managing the risks of new technologies, products, or delivery channels;

⁴⁵ Obligations with an asterisk (*) would only be required for cash transactions above the applicable threshold.

- assessing their money laundering and terrorism financing risks and develop a compliance programme, which would be required to be audited;
- taking additional steps to manage customers or transactions from higher risk countries;*
- reporting suspicious activities in all situations.

Requiring high value dealers to fully comply with the AML/CFT Act would address the issues we have identified, and it would also bring New Zealand more in line with FATF requirements. However, it would significantly increase compliance costs for these businesses. We would also need to navigate the fact that the FATF's requirements only relate to dealers in precious metals and stones, whereas our definition of high value dealers includes other types of dealers, such as motor vehicle dealers and art dealers.



- 4.210. Should we extend additional AML/CFT obligations to high value dealers? Why or why not? If so, what should their obligations be?
- 4.211. Should all high value dealers have increased obligations, or only certain types, e.g., dealers in precious metals and stones, motor vehicle dealers?
- 4.212. Are there any new risks in the high value dealer sector that you are seeing?

Other issues or topics

The AML/CFT regime does not operate in a vacuum, and there are many other systems, frameworks, and regimes that should be considered as part of ensuring the Act is fit-for-purpose and works effectively. We have identified several other issues or topics that overlap or intersect with the AML/CFT Act, or otherwise should be generally considered as part of the review.

Cross-border transportation of cash

Sections 68 to 71 of the Act set out requirements that apply in relation to movements of cash, including negotiable instruments (e.g., cheques), into or out of New Zealand. This includes physical transportation of cash and sending cash via mail or cargo. The primary obligation is that people cannot move cash into or out of New Zealand if it is equal to or more than NZD 10,000 without making a Border Cash Report (BCR). People who fail to declare, or declare the wrong amount commit an offence provided they do not have a reasonable excuse for failing to or declare or making a false declaration.

Unlike the rest of the AML/CFT regime, these sections apply to the general public and not specifically to businesses with AML/CFT obligations. The purpose of these sections is to ensure transparency of cross-border cash movements and deter people from not or falsely reporting cash movements.

When reports should be filed for unaccompanied cash

When cash is moved in an unaccompanied manner, a BCR is required before the cash leaves New Zealand or is received by a person in New Zealand. “Import” and “export” are not defined in the Act and Customs instead relies on the definitions of import and export in section 5 of the *Customs and Excise Act 2018*. Goods must pass the 12 nautical mile limit contiguous zone to become an export under this approach, but this can cause difficulties for Customs’ enforcement of BCR obligations where cash has been intercepted and seized before it has left Customs control and no report has been filed.

The Act could define “import” and “export” to address these challenges, rather than rely on the definitions in the *Customs and Excise Act 2018*. We could, for example, align these definitions with how Australia has defined import and export in section 57 and 58 of their AML/CFT Act 2006, and also set out how reports should be filed for unaccompanied cash (e.g., cash sent through the mail). This would clarify how the existing offence of failing to report applies with respect to unaccompanied cash and ensure a BCR is submitted alongside any Customs trade and mail declaration before the item leaves from or arrives into New Zealand.



- 5.1. Should the AML/CFT Act define the point at which a movement of cash or other instruments becomes an import or export?
- 5.2. Should the timing of the requirement to complete a BCR be set to the time any Customs trade and/or mail declaration is made, before the

item leaves New Zealand, for exports, and the time at which the item arrives in New Zealand, for imports?

- 5.3. Should there be instances where certain groups or categories of vessel are not required to complete a BCR (for example, cruise ships or other vessels with items on board, where those items are not coming off the vessel)?

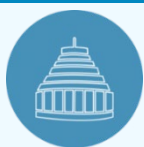
Sanctions for falsely declared or undeclared cash

The FATF recommends proportionate and dissuasive sanctions be applied in instances where cash movements above the threshold have been falsely declared or not declared at all. The Act currently allows for a term of imprisonment of up to three months or a fine of up to NZD 10,000 (or NZD 50,000 for bodies corporate or partnerships). However, the Act also allows for the chief executive of Customs to summarily dispose of false or undeclared cash by accepting a sum of NZD 500 from the person who failed to accurately declare the cross-border movement of cash. The FATF did not consider the penalty for summary disposal to be sufficiently proportionate or dissuasive and recommended change.

Recommended action (b) for Immediate Outcome 8, page 44

New Zealand should ensure that effective, proportionate, and dissuasive sanctions are applied for non-declared transportation of cash.

There are numerous ways we could ensure the penalty for false or undeclared movements of cash is proportionate and dissuasive. One option is to increase the overall penalty levels available in the Act to ensure that more serious conduct can be appropriately responded to. Another option would be to explicitly link the penalty (or portion of the penalty) to the amount of cash that has not been declared. A third way would be to replace the current penalty regime under [section 113](#) with an infringement regime to increase the immediacy of the penalty for those not complying.



- 5.4. How can we ensure the penalties for non-declared or falsely declared transportation of cash are effective, proportionate, and dissuasive?

Powers to search and seize cash to investigate its origin

Where cash is not declared or is falsely declared, Customs officers are able to seize the cash as it becomes a 'prohibited good' under the *Customs and Excise Act 2018*. However, these powers do not apply when the cash has been properly declared, unless the Customs officer forms a suspicion that the goods are an instrument of a crime or tainted property. The Act could be expanded to include a power, similar to an unexplained wealth order, which requires a person moving suspiciously large volumes of cash to prove that the cash has a legitimate origin and for the cash to be detained in the interim.



- 5.5. Should the Act allow for Customs officers to detain cash even where it is declared appropriately through creating a power, similar to an unexplained wealth order that could be applied where people are attempting to move suspiciously large volumes of cash?
- 5.6. If so, how could we constrain this power to ensure it does not constitute an unreasonable search and seizure power?

Other forms of value movement

The current BCR requirements only apply to movements of “cash”, which the Act defines to mean physical currency or bearer-negotiable instruments (e.g. cheques, bearer bonds, money orders). As such, movements of value across a border that do not involve currency or bearer-negotiable instruments do not require a BCR to be submitted. For example, BCRs are not required for movements of stored value instruments such as vouchers, casino chips, or precious metals and stones. This represents a potential vulnerability that could be exploited. However, requiring a BCR for other forms of value movement may present challenges for detection when moving them across the border, and also determining the amount of value being moved (e.g., the amount loaded on a stored value instrument or the value of precious metals or stones).



- 5.7. Should BCRs be required for more than just physical currency and bearer-negotiable instruments and also include other forms of value movements such as stored value instruments, casino chips, and precious metals and stones?

Privacy and protection of information

The Act requires businesses to collect a large amount of personal information from their customers, particularly where the risks are high, and businesses need to obtain and verify information relating to a customer’s source of wealth or source of funds. Some of this information is also required to be provided to the government automatically (e.g., for prescribed transaction reports) or upon request by a government agency. Information received can also be shared between agencies, but there are limits on when this can occur and the purposes for which information can be shared.



- 5.8. Does the AML/CFT Act properly balance its purposes with the need to protect people’s information and other privacy concerns? If not, how could we better protect people’s privacy?

Requiring mandatory deletion of financial intelligence

One area where we could adjust the balance between the Act’s purposes and the Privacy Act 2020 is with respect to how long the FIU or other agencies can hold information, including financial intelligence. There is no retention period specified in the Act for information held by government agencies, but we could include one for some types of information. In particular, the Act could specify that prescribed transaction reports (which indiscriminately collect personal

information relating to cash transactions and international wire transfers) must be deleted after a certain period.



- 5.9. Should we specify in the Act how long agencies can retain information, including financial intelligence held by the FIU?
- 5.10. If so, what types of information should have retention periods, and what should those periods be?

Legally privileged information

In various circumstances, the Act allows people to refuse to disclose information or documents on the ground that it contains privileged communication. This includes reporting suspicious activities, prescribed transactions, and providing information upon request from an AML/CFT supervisor or the FIU. “Privileged communication” is defined in [section 42](#), and there is a process set out in [section 159A](#) for testing whether a document or information is, in fact, privileged.



- 5.11. Does the Act appropriately protect the disclosure of legally privileged information? Are there other circumstances where people should be allowed not to disclose information if it is privileged?
- 5.12. Is the process for testing assertions that a document or piece of information is privileged set out in [section 159A](#) appropriate?

Harnessing technology to improve regulatory effectiveness

Innovative skills, methods, and processes, as well as innovative ways to use technology, can help regulators, supervisors, and businesses overcome many challenges associated with AML/CFT. Technology can facilitate data collection, processing, and analysis, and help businesses identify and manage money laundering and terrorism financing risks more accurately and quickly.

Internationally and domestically many technology-based solutions have been developed. Domestically, various providers offer digital identity verification systems to assist with CDD processes, as well as solutions for account and transaction monitoring. Internationally, businesses have been able to make use of artificial intelligence and machine learning, as well as natural language processing and application programme interfaces to improve AML/CFT effectiveness. Regulators and agencies can also use technology to better support regulatory outcomes and engagement, particularly with analysing financial intelligence and other information received from businesses.

We want to understand what challenges and barriers currently exist that prevent businesses from harnessing technology to improve regulatory outcomes. The FATF has identified that technological innovation requires more technology-active regulators, forward-looking supervision,

and evolving regulatory guidance.⁴⁶ The FATF also notes that increased communication and cooperation between the public and private sector is key to setting up and promoting a more technology enabling regulatory environment and contribute to overcoming identified operational challenges.

Other potential challenges identified by the FATF include:

- being able to explain new technologies to supervisors and for supervisors to properly be able to interpret the results can be key to securing support for the tools;
- regulators and supervisors can be slow to adjust regulatory practices to accommodate or promote adoption of new technologies;
- the absence of standardised data that developers can use to integrate into their tools, can be easy to understand and explain to non-experts, and easy to communicate to counterparts and regulators when needed;
- data is often not harmonised within countries or across borders, which can increase the cost of investing in new technologies if systems require fine tuning to accommodate different country requirements;
- an absence of additional guidance for how to interpret current domestic and international recommendations in the digital era;
- uncertainty as to who should be responsible for scrutinising the vendors of tools and the tools themselves (private sector or supervisors, or both);
- the effectiveness of new technologies to improve outcomes has not been properly assessed internationally or domestically, which could impact both the adoption of technology as well as technological developments.



5.13. What challenges or barriers have you identified that prevent you from harnessing technology to improve efficiencies and effectiveness? How can we overcome those challenges?

Enabling the adoption of digital identity

As part of the Government's Digital Identity Programme, Cabinet agreed to establish a Digital Identity Trust Framework. The Framework will set out the rules for how digital identity services can be delivered, including accreditation, legal enforcement, and governance, to enable the development of a secure and sustainable digital identity ecosystem.

We consider that the AML/CFT regime could be a prime candidate for making use of the digital identity framework and ecosystem, and we want to ensure that the regime is set up in a way to enable digital identity to be adopted once the framework is operational. While we do not have the full details about how the Framework will operate, we are interested in your views about whether there are any additional challenges that we should resolve to enable adoption when the time comes.

⁴⁶ FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021), available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>



- 5.14. What additional challenges or barriers may exist which would prevent the adoption of digital identity once the Digital Identity Trust Framework is established and operational? How can we overcome those challenges?

Harmonisation with Australian regulation

One of the considerations that Government had when developing the AML/CFT Act in 2009 was ensuring harmonisation, as much as possible, between our new proposed regime and existing Australian regulation. We recognised that many businesses operate in both Australia and New Zealand, and harmonising obligations would achieve greater efficiencies for businesses and government. However, we also need to ensure that our regulation is fit for New Zealand's risk and context, which is similar to Australia's but not exactly the same.



- 5.15. Should we achieve greater harmonisation with Australia's regulation? If so, why and how?

Ensuring system resilience

COVID-19 was a significant challenge for New Zealand in general, but also presented unique challenges for the AML/CFT system and tested its resilience. We had to rapidly adjust our understanding about money laundering and terrorism financing risks due to COVID-19 and communicate that to businesses. The change in risks was partly driven by novel opportunities for fraudulent behaviour as well as a dramatic change in how businesses interacted with their customers, meaning that previous measures were less effective at mitigating risks. In addition, agencies had to change how they supervised or monitored compliance with AML/CFT obligations, including how to conduct desk-based reviews and onsite inspections while New Zealand was in various levels of being locked down.

In general, AML/CFT agencies handled COVID-19 reasonably well and adjusted to the challenges to ensure the regime continued to operate. However, part of this may have been due to the relatively short lockdown periods in New Zealand. The AML/CFT system's resilience may have been pushed past breaking point had the lockdown periods been longer term. As such, we want to ensure that the system is resilient to challenges, both long and short term.



- 5.16. How can we ensure the AML/CFT system is resilient to long- and short-term challenges?

Minor changes

We have identified a number of minor changes that could be made to the Act or regulations. This section sets out the issue we have identified and our proposal for change. Changes that we can make to regulations are highlighted in yellow.



- 6.1. What are your views regarding the minor changes we have identified? Are there any that you do not support? Why?
- 6.2. Are there any other minor changes that we should make to the Act or regulations?

Definitions and terminology

| Issue | Proposal for change |
|---|--|
| Life insurer is not currently defined in the AML/CFT Act; however, the definition of life insurance policies is by cross reference to the Insurance (Prudential Supervision) Act 2010. | Define life insurer in the AML/CFT Act by reference to the Insurance (Prudential Supervision) Act 2010. |
| The meaning of the exclusion of “cheque deposits” in the definition of occasional transaction in section 5 of the AML/CFT Act is unclear. It is intended to apply to a deposit by cheque made at a bank or non-bank deposit taker, such that it does not trigger an occasional transaction by the person making the deposit with the bank. However, this is not specified. | Limit the exclusion of cheque deposits only to deposits made at a bank, non-bank deposit taker, or similar institution in line with the original policy intent. |
| The definition of a DBG allows a group of ‘related’ DNFBPs, and their subsidiaries, that are reporting entities (within the same sector), to form a DBG with each other. ‘Related’ is intentionally not defined and DIA as the supervisor has issued guidance to assist DNFBPs understand how this should be interpreted. The Act appears to currently require subsidiaries to also be reporting entities to join a DBG., which is not the policy intent. | Propose that a DBG may be formed amongst a group of related reporting entities within a DNFBP sector and may also include a subsidiary of one of those DNFBPs in New Zealand (that is not a reporting entity). |
| Section 114 of the AML/CFT Act is intended to convey the importance of the functions under the Customs and Excise Act 2018 in supporting the AML/CFT system but the current drafting does not clarify how the functions operate together. | Clarify and tidy up the sections to ensure the functions can clearly operate together. |

Information sharing

| Issue | Proposal for change |
|--|---|
| <p>Several key Acts are currently not included under <u>section 140</u> of the AML/CFT Act. This limits data and partnerships across agencies and is preventing full environment assessments. The key agencies responsible for the listed legislation have observed money laundering and other harms but are currently unable to share information with the AML/CFT agencies.</p> | <p>Issue regulations to include additional Acts within the scope of <u>section 140</u> to enable broader information sharing, such as: <i>Commerce Act 1986, Corrections Act 2004, Criminal Proceeds (Recovery) Act 2009, Defence Act 1990, Environment Act 1986, Immigration Act 2009, and Trust Act 2019.</i></p> |
| <p>Supervisors are empowered under <u>section 48</u> to disclose personal information relating to employees or senior managers for law enforcement purposes and for the purpose of detecting, investigating, prosecuting any offence under specific Acts. Some Acts are not listed which limit the ability for some information that AML/CFT agencies hold to be shared for other regulatory purposes.</p> | <p>Add the following Acts to <u>section 48(b)</u> to improve clarity of the section and enable appropriate information sharing: <i>Financial Markets Conduct Act 2013, Non-bank Deposit Takers Act 2013, Insurance (Prudential Supervision) Act 2010.</i></p> |
| <p>There are limited provisions explicitly allowing DIA to share information internally for law enforcement purposes (as defined in <u>section 5</u>). DIA administers other relevant legislation and it is not clear whether the AML/CFT function within DIA is able to share information with the teams responsible for the legislation listed above or vice versa.</p> | <p>Add further Acts to <u>section 137(6) & (7)</u> to clarify the ability for DIA to use information obtained as AML/CFT supervisor in other capacity and vice versa, e.g. <i>Passport Act 1992, Births, Deaths, Marriages and Relationship Registration Act 1995, Citizenship Act 1977.</i></p> |
| <p>There is no explicit provision in the AML/CFT Act which allows supervisors to conduct enquiries on behalf of foreign counterparts. <u>Section 132(2)(e)</u> of the AML/CFT Act provides a general power to initiate and act on requests from overseas counterparts, but not specifically conduct enquiries.</p> | <p>Clarify that supervisors are empowered to conduct enquiries on behalf of overseas counterparts.</p> |

SARs and PTRs

| Issue | Proposal for change |
|---|---|
| <p>No agency has the explicit function of ensuring compliance with SAR obligations. This function is not specifically listed as part of the functions of the AML/CFT Supervisors in <u>section 130</u> (but supervisors are required to monitor for compliance more generally). Similarly, the Commissioner of Police is empowered to provide feedback to reporting entities on the quality and timing of their SARs and enforce the requirement to report.</p> | <p>Clarify which agencies are responsible for supervising compliance with SAR obligations.</p> |
| <p>The requirements set out in regulations for prescribed transaction reports made for international wire transfers are unclear about whether the country noted should be where the account is held or the country of the originator.</p> | <p>Amend the regulation to obtain both the location of the account and the address of the sender to capture all relevant country information.</p> |

Exemptions

| Issue | Proposal for change |
|--|---|
| <p><u>Regulation 24AC</u> of the AML/CFT (Exemptions) Regulations 2011 exempts reporting entities from certain sections obligations when subject to a production order or order issued under <u>section 143(1)(a)</u>. However, reporting entities also receive orders under the Customs and Excise Act 2018 which may inadvertently lead to tipping off. In addition, in the process of complying with the relevant order, the reporting entity may form suspicions about associated persons. The exemption does not explicitly cover associates and therefore there is a risk that suspicious associates are tipped off.</p> | <p>Expand the exemption to also exempt reporting entities subject to an order issued under <u>section 251</u> of the Customs and Excise Act 2018 as well as in respect of any suspicious associates who are identified in the process of complying with the relevant order.</p> |
| <p><u>Regulation 17</u> AML/CFT (Exemptions) Regulations 2011 exempts reporting entities that are not an insurance company who are providing a service under a premium funding agreement from <u>section 14-26</u> of the AML/CFT Act but does not exempt them from the requirement to identify a customer under <u>section 11</u>. This means exempt reporting entities must conduct ongoing CDD and account monitoring under <u>section 31</u>, but as they have not conducted CDD they have nothing to review.</p> | <p>Link the exemption more directly to the level of ML/TF risk associated with premium funding and clarify intention (or not) to capture premium funding as an activity for the purposes of AML/CFT</p> |
| <p><u>Regulation 22</u> of the AML/CFT (Exemptions) Regulation 2011 exempts debt collection services from the AML/CFT Act other than relating to suspicious activity reporting. Debt collection services are defined as “the collection of debt by a person other than the creditor to whom it is owed or, where it has been assigned, to whom it was originally owed”. The scope of this definition is unclear.</p> | <p>Clarify that the definition of debt collection services only relates to the collection of unpaid debt rather than the collection of any funds owed by one person to another.</p> |
| <p><u>Regulation 9</u> of the AML/CFT (Exemptions) Regulations 2011 currently exempts currency exchange transactions performed in hotels that do not exceed NZD 1000 from most obligations in the Act, except obligations to file suspicious activity reports and keep records of any reports filed. However, the way this exemption operates may cause confusion for hotel operators which could be exploited by people seeking to launder money or finance terrorism. In particular, hotel operators may not be aware that they have full obligations for any currency exchange transaction that exceeds NZD 1000, irrespective of how regularly they engage in any large value currency exchange transaction.</p> | <p>Clarify that the exemption applies to hotel providers which only undertake currency exchange transactions below NZD 1000.</p> |
| <p><u>Section 158</u> states that the Minister of Justice must consult with the Ministers responsible for the AML/CFT supervisors and any other appropriate persons before deciding on a Ministerial exemption.</p> | <p>Specifically include the FIU NZ Police in the list of agencies/roles that the Minister must consult with when considering a Ministerial exemption.</p> |

Offences and penalties

| Issue | Proposal for change |
|--|--|
| AML/CFT supervisors can issue a formal warning for failure to comply with AML/CFT requirements. However, calling these “formal warnings” does not necessarily carry the intended weight with the sector. | Replace “Formal warnings” with “Censure” to indicate the weight of the action. Censure is much more than a warning and includes a mandatory action plan. |
| There are two civil liability acts not explicitly included in section 78 of the Act. These are 1) failing to submit a suspicious activity report; 2) failures in respect of a risk assessment. ⁴⁷ It is also currently unclear whether 3) failing to submit an annual report to an AML/CFT supervisor is a civil liability act. | Amend section 78 to include these compliance breaches as civil liability acts. |

Preventive Measures

| Issue | Proposal for change |
|---|---|
| Businesses are required to “have regard” to the factors set out in section 58(2) when conducting a risk assessment. This includes any applicable guidance material produced by AML/CFT supervisors or the Police, such as the National Risk Assessment or the various sectoral risk assessments. However, the language of “have regard to” could allow businesses to consider, but ultimately reject, government advice about national or sectoral risks and therefore fail to implement appropriate controls. | Amend section 58(2) to ensure that a business’ risk assessment reflect government advice about national and sectoral risks. |
| In various sections of the AML/CFT Act, where a requirement for CDD is triggered outside a business relationship, there is reference to a customer seeking to conduct an occasional transaction or occasional activity. A person (outside a business relationship) becomes a customer if they conduct or seek to conduct an occasional transaction or occasional activity. | Replacing the term ‘customer’ with ‘person’ in sections 14(1)(b) , 18(1)(b) , 22(1)(b) , 22(1)(b)(ii) , 22(2)(b) , and 22(5)(b) to align with the definition of customer in section 5 . |
| Businesses do not have an explicit obligation to verify any new information obtained through ongoing CDD, except where enhanced CDD is triggered. | Issue a regulation which explicitly requires businesses to verify any new information obtained through ongoing CDD. |
| Regulation 10 of the AML/CFT (Requirements and Compliance) Regulations 2011 require reporting entities to obtain information about the existence and name of any nominee directors and nominee shareholders. However, the definition of “nominee director” can include situations where directors of subsidiary companies or joint venture companies are required or accustomed to follow the directions from the holding company or appointing shareholder. This arrangement was not intended to be captured by the additional requirements. | Amend the definition of nominee director to exclude instances where the director is required to accustomed to follow the directions of a holding company or appointing shareholder. |

⁴⁷ *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited* [2017] NZHC 2363, at [5]. *Department of Internal Affairs v Qian Duoduo Limited* [2018] NZHC 1887, at [3].

| Issue | Proposal for change |
|---|---|
| <p><u>Section 37</u> applies prohibitions if a reporting entity “is unable to” conduct CDD in accordance with the AML/CFT Act. One reading of this is that if a reporting entity can conduct CDD as required, but merely chooses not to, the prohibitions do not apply.</p> | <p>Replace “is unable to” with “does not” in <u>section 37</u> to ensure the prohibitions apply in all appropriate instances where CDD is not conducted.</p> |
| <p>Simplified CDD is intended to apply only in situations where there are proven lower risks. There is no explicit requirement for businesses to not apply simplified CDD measures where there are higher risks, including where there is a suspicion of money laundering or terrorism financing.</p> | <p>Issue a regulation which states that simplified CDD is not appropriate where money laundering or terrorism financing risks are high or if there is suspicion of ML/TF.</p> |
| <p>Businesses are not required to keep records of prescribed transaction reports.</p> | <p>Issue a regulation which requires businesses to keep records of prescribed transaction reports for five years.</p> |
| <p><u>Section 52</u> of the Act states that records must be kept in written form in English or in a form to make them readily available. This means, but does not explicitly state, that records must be available immediately, or upon request.⁴⁸</p> | <p>Amend <u>section 52</u> to clarify that records must be made available immediately (e.g. upon request from a supervisor).</p> |
| <p>The Act does not set out how long businesses should retain account files, business correspondence, and written findings.</p> | <p>Issue a regulation which requires businesses to retain account files, business correspondence, and written findings for five years.</p> |
| <p>There is no requirement that copies of records must be stored in New Zealand, particularly copies of customer identification documents.</p> | <p>Issue a regulation which requires businesses to retain copies of records in New Zealand to ensure they can be easily accessible when required.</p> |
| <p>There is currently no requirement for ordering institution to maintain records about beneficiary’s account number or unique transaction reference number.</p> | <p>Require ordering institutions to keep records on beneficiary account number or unique transaction numbers.</p> |
| <p>It is currently not clear that wire transfer obligations apply to an underlying customer for MVTs providers that use agents.</p> | <p>Issue a regulation stating that the originator or beneficiary of a wire transfer is the underlying customer, not the MVTs provider’s agent.</p> |
| <p>There is a current Ministerial exemption in place that enables members of a DBG (that are reporting entities) to share a compliance officer, subject to certain conditions. The intent is to reduce compliance burden across members of a DBG.</p> | <p>Amend the Act to allow members of a DBG to share a compliance officer.</p> |

⁴⁸ *Department of Internal Affairs v OTT Trading Group Limited, Tonghui Qi and Lee Chon Woon* [2020] NZHC 1663, at [76], [77] and [78].

Index of terms

- beneficial owner
 - definition, 54
 - person on whose behalf a transaction is conducted (POWBATIC), 55
 - process for legal arrangement customers, 57
 - process for legal person customers, 56
 - ultimate ownership or control, 55
- Bitcoin. *See* virtual asset service providers
- border cash reporting, 101–3
 - sanctions, 102
 - search powers, 102
 - unaccompanied cash, 101
- compliance costs, 6, 17, 20, 23, 24, 25, 26, 27, 28, 29, 30, 31, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 60, 61, 62, 63, 68, 70, 74, 77, 78, 83, 85, 86, 91, 95, 100
- compliance programme, 92
 - compliance officers, 93
 - group-wide programmes, 93
 - review and audit requirements, 94
- compliance programmes
 - independent auditors, 40
- Correspondent banking, 75
- Crown entities and agents, 33
- cryptocurrencies. *See* virtual asset service providers
- customer due diligence, 47–65
 - address verification, 58
 - definition of customer, 48
 - digital identity, 105
 - enhanced CDD, 50, 52, 64
 - enhanced CDD measures, 59
 - large organisations, 60
 - new reliance provisions, 92
 - ongoing CDD, 61
 - pre-Act customers, 63
 - real estate, 49
 - reliance, 89–92
 - reliance on approved entities, 90
 - simplified CDD, 50, 52
 - standard CDD, 50, 51
 - third party reliance, 91
 - tipping off, 64
 - trusts, 61
- DBG
 - approving formation, 40
 - eligibility criteria, 90
 - financial groups, 94
 - including subsidiaries, 107
 - overseas members, 91
 - reliance, 89, 90
 - shared compliance officer, 111
- de-risking, vi, 2
- DNFBPs
 - criminal defence lawyers, 26
 - ordinary course of business, 19
 - prescribed transaction reporting, 86
- exemptions, 30
 - community trusts, 33
 - Crown entities and entities, 33
 - internet auction providers, 31
 - non-finance businesses, 32
 - pawnbrokers, 23
 - process, 5
 - regulatory exemptions, 32
 - remittance card facilities, 31
- FATF standards
 - address verification, 59
 - beneficial ownership, 55, 56
 - combatting proliferation financing, 2
 - compliance officers, 93
 - customer due diligence, 50, 52, 53, 59, 64
 - DNFBPs, 19, 25
 - MVTS, 77
 - non-profit organisations, 29
 - politically exposed persons, 69
 - real estate, 49
 - reliance, 90
 - sanctions for senior managers, 44
 - targeted financial sanctions, 3, 72
 - virtual asset service providers, 27, 80
 - wire transfers, 81, 83, 84, 85
- financial inclusion, 8
- government powers
 - approving DBGs, 40
 - freezing or stopping transactions, 11
 - ongoing monitoring of accounts or transactions, 10
 - requesting information from other businesses, 10
 - supervising TFS, 11
 - supervisors, 39
- high value dealers, 24, 99
 - cash reporting threshold, 88
 - definition, 23
 - obligations, 99
 - online marketplaces, 31

- ordinary course of business, 23
- pawnbrokers, 23
- risk understanding, 99
- suspicious activity reporting, 99
- higher-risk countries, 95
 - countermeasures, 96
 - countermeasures against specific individuals and entities, 97
 - FATF requirements, 96
 - understanding country risk, 95
- information sharing
 - about employees or senior managers, 108
 - data matching, 15
 - direct data access with the FIU, 14
 - from other legislation, 108
 - group wide programmes, 93
 - inquiries on behalf of foreign counterparts, 108
 - suspicious activity reports, 98
 - within DIA, 108
- insurers
 - CDD on beneficiaries, 53
 - obligations for non-life insurance policies, 26
 - politically exposed persons, 70
- MVTS providers, 76–78, 87
 - list of agents, 77
 - remittance card facilities exemption, 31
 - responsibility for agents, 77
 - SAR obligations, 99
 - sub-agents, 78
- new technologies, 78–79
 - digital identity, 105
 - harnessing to improve effectiveness, 104
 - risk assessment, 79
 - risk mitigations, 79
 - virtual assets, 27
- nominee
 - definition of nominee director, 110
 - director or shareholder, 25, 32
 - real estate, 50
- non-bank financial institutions, 86
- non-profit organisations, 29
 - obligations, 30
 - unintended consequences, vi, 7
 - vulnerabilities, 30
- occasional transactions
 - cheque deposits, 107
 - stored value instruments, 24
 - use of customer, 110
 - virtual assets, 80
- offences and penalties, 42, 110
 - application to directors etc, 44
 - higher end, 44
 - intermediate options, 43
 - liquidation following non-payment, 45
 - liquidation time limit, 45
- pawnbrokers. *See* high value dealers
- politically exposed persons, 66–71
 - definition, 67
 - foreign PEPs, 68
 - mitigating the risks of, 70
 - time limit, 67
- prescribed transaction reporting, 85–89, 85
 - applicable threshold, 88
 - DNFBP obligations, 86
 - intermediary institutions, 87
 - MVTS providers, 87
 - obligations, 86
 - reasonable timeframe, 88
 - threshold, 24
 - types of transactions, 86
- private sector
 - engagement with Government, 9
 - role of, 8
- proliferation financing
 - assessing risks of, 2
 - purpose of the Act, 2
 - targeted financial sanctions, 3
- PTRs. *See* prescribed transaction reporting
- purpose of the Act, 1
 - combatting proliferation financing, 2
 - implementing TFS, 3
 - prevent money laundering and terrorism financing, 1
- real estate
 - customer, 49
 - managing funds, 51
 - risks, 49
 - timing of CDD, 49
- record keeping, 65
 - third party reliance, 91
 - use of agents, 42
- reliance, 89–92
- remitters. *See* MVTS providers
- risk-based approach, 4
 - life insurance, 54
 - non-profit organisations, 30
 - politically exposed persons, 68
 - trusts, 61
 - understanding risks, 4
 - wire transfer policies, 84, 85
- search powers
 - border cash movement, 102
 - inspections at dwellinghouses, 39
 - remote inspections, 39

- secondary legislation
 - annual reports and forms, 13
 - Code of Practice, iv, 12, 13, 57, 60, 74, 86
 - powers, 12
 - rules, 13
- stored value instruments, 24
 - border cash reporting, 103
 - non-tangible stored value instruments, 25
- suspicious activity reporting, 97
 - CDD obligations, 64
 - high value dealers, 99
 - quality of reports, 97
 - relying on DBGs, 90
 - sharing SARs, 98
 - supervisory agency, 108
 - TFS, 74
 - tipping off, 64
 - use of agents, 42
- Targeted financial sanctions, i, *See* TFS
- TBML. *See* trade-based money laundering
- TCSPs
 - acting as company secretary, 25
 - definition, 21
 - managing funds in trust accounts, 51
 - politically exposed persons, 68
 - territorial scope, 34
- terminology, 19
 - engaging in or giving instructions, 22
 - financial institution, 22
 - financial institution activities, 21, 22
 - in the ordinary course of business, 23
 - managing client funds, 21
 - multiple types of activities, 20
 - ordinary course of business, 19
 - sums paid as fees for professional services, 21
- territorial scope, 34
- TFS
 - AML/CFT programme, 72
 - assurance, 75
 - freezing without delay, 75
 - identifying associates or people acting on behalf of, 73
 - implementation, 71–75
 - implementation as a purpose, 3
 - notification of actions taken, 74
 - notification of designations, 73
 - proliferation financing risk, 72
 - risk assessment, 72
 - screening for designations, 74
 - supervision of, 11
 - suspicious activity reporting, 74
 - suspicious property reports, 74
- trade-based money laundering, 28
 - data matching, 15
 - preparing annual accounts and tax statements, 29
 - preparing or processing invoices, 28
- trust and company service provider. *See* TCSP
- trusts
 - acting as trustee, 32
 - beneficial ownership, 57
 - CDD obligations, 48
 - community trusts, 33
 - enhanced CDD, 61
 - trust accounts, 51
 - trustee company, 32
- unintended consequences, vi, 2, 7, 8, 20
 - address verification, 58
 - de-banking. *See* de-risking
 - de-risking, 7, 16
 - financial inclusion, 8, 58
- VASPs. *See* virtual asset service providers
- virtual asset service providers, 80–81
 - capture, 27
 - CDD obligations, 80
 - obligations, 80
 - occasional transactions threshold, 80
 - wallet providers, 27
 - wire transfers, 81
- wire transfers, 81–85
 - applicable threshold, 82
 - beneficiary institution, 85
 - definitions, 81
 - exemption, 87
 - high-risk transactions, 83
 - intermediary institutions, 84
 - MVTS, 87
 - ordering institution, 82
 - virtual assets, 81

Ministry of Justice
Tāhū o te Ture

justice.govt.nz

info@justice.govt.nz

0800 COURTS
0800 268 787

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

