aml

From: [redacted]@financialbarrister.com
Sent: Friday, 17 December 2021 5:08 pm
To: aml
Cc: [redacted]
Subject: Submissions of AML/CFT Act review
Attachments: Submissions in response to AML CFT Act Consultation Document October 2021 17 December 2021.pdf

Dear Nick

Attached is our final submission. Please disregard [redacted] prior emailed attachment.

We would be happy to present our submissions in person, or be involved in the focus group established for the next round of the review.

We appreciate the extension you have provided to us to complete our submissions. It is a thorough review, and so a large amount of material to work through.

Kind regards

[redacted]

[redacted]
BARRISTER

LLB BCom

T [redacted]

A Regent Chambers
Level 4, 68 Shortland Street
Auckland City 1010
W www.financialbarrister.com

Submissions to the Strategic Review of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

December 2021

Important notice

The contents of this document must not be construed as legal or compliance advice. The authors do not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken because of reading, or reliance placed on the authors because of having read, any part, or all, of the information in this response document or for any error, inadequacy, deficiency, flaw in or omission from the discussion document.

Glossary of terms

The terms used in this document are the same used by the Ministry of Justice (**MOJ**) in its consultation document of the review of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (**AML/CFT Act or the Act**) dated October 2021.

About the Authors

Merran Keil

Merran is an experienced litigator specialising in resolving business, financial markets (securities), contractual, fair trading, insurance and negligence disputes. Merran has acted for a wide range of clients; individuals, businesses and the government, in Court claims, appeals, mediation, judicial review, and tribunal proceedings. She has also acted for reporting entities that have had AML/CFT supervisors' inquiries or investigations conducted in respect of their compliance with the Act.

Uddhav Kirtikar

FMA Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) establishment team.

While at FMA, Uddhav played a key part in establishing the AML/CFT regime in New Zealand. He was FMA's lead writer for several AML/CFT Act guidance papers that supervisors published. Uddhav also designed the templates and processes that FMA used when it commenced its AML/CFT supervisory work.

Personal information and confidentiality

The authors consent to this submission being publicised.

Introduction

This joint submission is a response to some of the questions raised by MOJ in its strategic review of the AML/CFT Act.

The submissions are based on 20 years (collectively) of working with the AML/CFT Act as FMA staff members and working with reporting entities to assist them to meet their AML/CFT Act compliance obligations.

A "gold standard" AML/CFT regime is one which:

- maintains New Zealand's status as having a high quality and effective regime for discouraging money laundering and terrorism financing;

- does not compromise on the ease of doing business or unduly impacting the lives of New Zealanders, and
- contains sufficient tools to enable flexibility and ensure the regime responds to changing risks and new opportunities for addressing harm.

It is submitted that this review should focus these primary three factors.

The consultation document asks for submission on several potential amendments to the AML/CFT Act. However, the document does not include any indicative costs to reporting entities from the suggested amendments.

Any potential costs to reporting entities and barriers that they might raise to ease of business and access to essential services must be known to enable an informed submission.

Additionally, the review should consider how the current AML/CFT Act and regulations have:

- reduced crime in New Zealand and helped in preventing financing of terrorism in New Zealand or overseas; and
- contributed to increasing the public's confidence in the financial system.

The consultation document indicates that little or no consideration has been given to making amendments that result in:

- Increasing ease of access to essential financial, legal, and accounting services; or
- Reduction in the predicate offending that generates illegal funds that require laundering.

These secondary 4 factors should also guide the review.

Part 1 Consultation questions: Purpose of the AML/CFT Act

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?

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?

Our observations and submissions

The Act's purpose is to legislate for:

- the measures set out in the FATF Recommendations 10 – 23;
- how supervisors will monitor compliance and penalise non-compliance; and

- enhance NZ's reputation internationally as being a difficult country in which undertake ML and TF.

  The Act's purpose is to legislate what is required of financial institutions and designated sectors to prevent money laundering and financing of terrorism (**ML/FT**) [as set out in the FATF Recommendations (Updated June 2021)]. It is submitted that the prevention measures set out in the Recommendations are relatively simple.

  The Act and Codes of Practice should not be used to abdicate government responsibility for detection of predicate offences, nor should it burden reporting entities or their customers to carry out compliance that results in unreasonable costs relative to the service provided by any reporting entity.

  The FATF Recommendations require that reporting entities apply preventive measures, they do not require reporting entities to investigate, detect or deter ML/TF, nor operate in an atmosphere of distrust of their customers. The 'prevention' mechanisms stipulated by FATF is a requirement of reporting entities to *know their customers*.

  Detection and deterrence of crime and terrorism is the role of authorities under separate pieces of Legislation (including for example, the Crimes Act, Criminal Proceeds (Recovery) Act 2009 and the Terrorism Suppression Act 2002). For that reason, the wording of the Act's purpose is not a true reflection of how the Act should be framed, as detection and deterrence misplaces government responsibility on the private sector.

  Public confidence in the financial sector is enhanced when financial institutions are transparent and do not pass on private and confidential information to the police merely on the suspicion of a crime being involved in the funds' generation.

  However, as currently drafted and enforced by the supervisors, the Act requires reporting entities, under the threat of penalty, to collect information from the public and to pass on that private and confidential information to the police, merely on a suspicion that the funds might be linked to criminal activity.

  The Act's purpose of preventing ML and TF does not enhance the public's confidence in the financial system, when their own personal information is collected and not used transparently. Accordingly, it is illogical to stipulate that public confidence is a central purpose. Rather, its purpose is to enhance NZ's reputation internationally as a country that complies with FATF's recommendations.

  Money that requires laundering is generated only when the government's law enforcement agencies responsible for crime prevention are unable to detect the predicate offending. Terrorism is financed when there is a failure of the government's counter terrorism agencies. ML and TF are crimes under the Crimes Act and the Terrorism Suppression Act. Reporting entities pay for law enforcement and intelligence activities through their taxes. Using legislation to require business to become confidential informants to law enforcement agencies, at their own (and the public's) cost is not at the centre of a high quality and effective regime for

discouraging money laundering and terrorism financing. What is central to an effective regime is allowing reporting entities to satisfy themselves (using flexible criteria to allow for varying customer relationships) that *they know their customer*.

Therefore, it is submitted that detection and deterrence of ML/TF is not central to the Act's purpose. The tenet of FAFT's recommendations is that reporting entities should know their clients. This is the primary purpose of the Act and should be stipulated in the Act's purpose.

Consultation questions: Combatting proliferation financing

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?

1.5 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?

Our observations and submissions

Weapons of mass destruction are developed by countries such as, New Zealand's major trading partners, the USA and the People's Republic of China.

Action against Iran appears to be linked to the political differences that the current regime has with the USA. There is a difference of opinion between the US and its allies in the EU over Iran's WMD programme and its proliferation.

There is currently sufficient sanction legislation that prohibits New Zealand business from dealing with countries sanctioned by the UN.

We have not come across any information in the public domain that would show that the police currently have a unit that actively prosecutes people for being involved in the proliferation of WMDs.

Requiring reporting entities to incur additional costs to pass on intelligence to the police on the financing the proliferation of WMDs will be manifestly disproportionate to the government's own investment in deterring and preventing the proliferation of WMD.

Therefore, we submit that the purpose of the Act should not be expanded to seek to counter the financing of proliferation of WMD [See also our observations in respect of TFS at 1.6, 1.34 and 4.103].

Consultation questions: Supporting the implementation of targeted financial sanctions

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

Our observations and submissions

Financing of terrorism is already criminalised. There is also legislation that criminalises dealing with sanctioned entities.

The Act requires reporting entities to make suspicious activity reports (**SAR**) to the FIU for activities that might be prohibited under the Terrorism Suppression Act.

We submit that expanding the Act to put in place additional TFS obligations is unnecessary, where there is no evidence the Act's obligation of knowing whether a customer's country has sufficient AML/CFT measures in place is insufficient to identify persons subject to such sanctions.

The 'knowing your country' obligation currently requires a reporting entity to assess whether a non-resident customer's country is:

- **Subject to international sanctions, embargos or other measures;**
- **Identified by FATF as a high risk or monitored jurisdiction; or**
- **Recognised as having supporters of terrorism or financing terrorism.**
  [See also our observations in respect of TFS at 1.4, 1.34 and 4.103]

Consultation Questions: Balancing prescription with risk-based obligations

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?

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?

Our observations and submissions

The legislation is currently risk based. It relies on the reporting entity to assess its ML/FT risks and then put in place an AML/CFT programme to deter and detect ML/FT occurring.

The currently has sufficient measures that enable a reporting entity to put in place a risk-based AML/CFT Act compliance regime. A business knows its risks better than its supervisor.

In our experience, supervisor staff lack operational knowledge of how reporting entities conduct their businesses, what the real risks of AML/CFT of those businesses are and are inconsistent in their interaction with reporting entities when conducting their supervisory tasks.

Therefore, we submit that there should be restrictions on supervisors' powers to impose their own assessments on a reporting entity or make directions to the same effect.

Consultation questions: Managing unintended consequences

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?

Our observations and submissions

The un-intended consequence of de-risking

Reserve Bank of New Zealand (**RBNZ**) has not issued guidance to Banks with regards to their AML/CFT Act compliance obligations when they establish a business relationship with another reporting entity, such as remittance businesses registered on New Zealand's Financial Service Provider Register (**FSPR**).

Unfortunately, the denial of banking services has occurred where New Zealand residents have been assessed by a Bank to be non-compliant with the Act. However, it is not for a Bank to pass judgment on another resident's compliance with the Act. The requirement under the Act to consider a customer's AML/CFT measures is only when that customer is non-resident (s 22(1) (a)(ii) of the Act).

There are currently sufficient provisions under the Act to prevent de-risking. For example, publishing a code of practice or guidance for the banking sector. Further, RBNZ has sufficient directing powers under the Reserve Bank Act to prevent de-risking.

We also submit that the current barriers to access services that some groups of people living in New Zealand might face due to the AML/CFT Act are because of the overly onerous and unlegislated obligations stipulated in Explanatory Notes to the Identity Verification Code of Practice **(IVCOP)**[more on this below].

We submit that there is cause for review of guidance, the IVCOP and its explanatory notes to make it clear that the denial of services to NZ resident customers (or potential customers) merely because a Bank believes that the customer (who is itself a reporting entity) has insufficient ML/TF safeguards in place is no reason to deny services. This is because it is the supervisors who

monitor compliance and the Court that determines whether a reporting entity is compliant (or not), not the Banks.

Consultation questions:

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?

Our observations and submissions: The role of the private sector; Partnering in the fight against financial crime

The private sector is in business primarily to earn profits, from which taxes are paid. Reporting entities are not in business to help the government prevent or prosecute criminal activity. The private sector already pays, through taxes, the government to prevent and prosecute crime.

Any collaboration that the government seeks with the private sector to assist it perform functions for which it funds from taxes, should not cost the private sector additional resources. Further the costs must not be directly or indirectly passed on to the public. Who will bear the cost of the private sector being forced to act as an extension of the police? Could the costs be met from recoveries under the Criminal Proceeds (Recovery) Act?

We submit that any collaboration that the government wishes to enter with the private sector to prevent crime should be voluntary. The government should not impose additional costs on the private sector to help it fulfil its core law enforcement role.

Information that the New Zealand public provide reporting entities must not be shared with any third parties without reasonable grounds and consistently with s 21 of the New Zealand Bill of Rights Act (NZBOR) and the Search and Surveillance Act 2012.

Statistical information about actions (or inaction) taken by the FIU as a result of SARs or PTRs would assist reporting entities in understanding whether their reports are being acted on appropriately.

Consultation questions: Helping to ensure the system works effectively

1.27 Should the Act 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?

Our observations and submissions

There is currently no mechanism for reporting entities to complain about actions by a supervisor and/or staff working for them.

The Office of the Ombudsman does not have the experience or skills required to investigate conduct that would amount to regulatory overreach by a supervisor.

We submit that an independent authority to which reporting entities can complain about the actions of a supervisor or staff working for a supervisor is necessary.

Such an authority will ensure that complaints are independently investigated. The authority must have sufficient powers to impose remedies against supervisors found to be acting outside the powers granted to them under the AML/CFT Act.

Consultation questions: Powers of the Financial Intelligence Unit

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?

Our observations and submissions

The police have wide information gathering powers under the Search and Surveillance Act and other legislation such as the Crimes Act, Terrorism Suppression Act and Misuse of Drugs Act. Limits on information gathering powers in those Acts have been tested through the Courts, when balanced against the NZBOR. The inclusion in the Act of information gathering powers over non-reporting entities is unnecessary.

We submit that no additional powers should be provided to the Financial Intelligence Unit of the New Zealand Police under the AML/CFT Act.

Consultation questions: Providing for ongoing monitoring of transactions and accounts

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?

Our observations and submissions

It is surprising that the government wishes to increase the public's confidence in the financial system and yet want to give powers to the police that could result in the abuse of trust that the public place in the financial, legal, accounting or other captured activity service providers.

The Police already have significant powers to investigate crime.

We submit that there should be no attempt by the government to provide information gathering powers to the FIU outside the provisions of the Search and Surveillance Act 2012.

Consultation questions: Freezing or stopping transactions to prevent harm

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?

Our observations and submissions

Harm has occurred when the predicate offence is successfully conducted, and funds generated.

The Police have powers under the Criminal Proceeds (Recovery) Act (**CPRA**) to act quickly in without notice proceedings to (restrain) freeze funds and transactions. Any harm that might come to the public will be from the predicate crimes that generate the illegal funds and the application of those funds to finance further

crime, therefore the powers of restraint will have the immediate effect of frustrating further criminal offending.

It is submitted that it is better use of resources for the police to concentrate their efforts on preventing the predicate crimes that generate illegal funds, than seeking powers that already exist under the CPRA.

How will freezing a criminal's funds not tip them off about the possibility of a criminal investigation?

What protection do reporting entities have from criminals whose activity they are forced to report to the police?

We submit that no additional powers be given to the FIU under the AML/CFT Act. The police have sufficient powers under existing legislation.

Consultation questions: Supervising implementation of targeted financial sanctions

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?

Our observations and submissions

A reporting entity cannot conduct business with a customer in a sanctioned country/ entity. A reporting entity that conducts business with a sanctioned country/ entity can be prosecuted.

We submit that enacting legislation to force reporting entities to enforce TFS could result in significant compliance costs. The government should not require reporting entities to assist it perform its law enforcement functions.

[See also our observations in respect of TFS at 1.4, 1.6 and 4.103]

Consultation questions: Codes of Practice

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?

Our observations and submissions

A code of practice under the Act is a statement of practice that will assist reporting entities to meet their obligations under the AML/CFT Act.

Whilst a code of practice could be a useful tool for business, the IVCOP is far from a useful tool. It adds compliance obligations that are not legislated.

For example, the IVCOP limits which government departments are reliable and independent for the purpose of s 13 of the Act. It also limits the types of government issued documents that can be used to verify the person's identity.

Codes of practice should not compromise the ease of doing business or unduly impacting the lives of New Zealanders. The requirement for businesses to demonstrate they are complying through some equally effective means indicates that the code of practice has gone through the same scrutiny as the legislation to which they apply. That is not the case.

The requirement for business to inform supervisors of their decision not to adopt the IVCOP has resulted in reporting entities being warned of consequences if they opt out of the IVCOP.

The below sets out the issues with the current IVCOP.

Section 15 of the Act requires a reporting entity to obtain the following information when conducting standard CDD:

- the person's full name;
- the person's date of birth;
- if the person is not the customer, the person's relationship to the customer;
- the person's address or registered office;
- the person's company identifier or registration number; and
- any information prescribed by regulations.

There are currently no regulations that require reporting entities to obtain any additional information other than that which is set out under s 15 of the Act. Reasonable steps must be taken to verify the information obtained under section 13.

As specified under s 13 of the Act, the reporting entity must verify this information on:

- the basis of documents, data or information issued by a reliable and independent source; or

- any other basis applying to a specified situation, customer, product, service, business relationship or transaction prescribed by regulations.

There are no regulations made under the Act that set out additional basis for verifying identity under s 13. Section 13 requires the source who has issued the document, data or information used to verify identity to be reliable and independent. There are no other requirements.

The IVCOP only permits certain documents that have the person's photograph on them to be used on their own to verify their name and date of birth. This requirement is not in the AML/CFT Act.

We note that the IVCOP does not allow the use of the following documents on their own:

- A New Zealand birth certificate;
- A New Zealand citizenship certificate; and
- A New Zealand Drivers Licence (**NZDL**).

Under the New Zealand Government Evidence of Identity Document, a New Zealand birth certificate and citizenship certificate are acceptable on their own to verify a person's name and date of birth.

We also note that a NZDL is issued to a person by the government. Therefore, it meets the requirements of s 13 of the AML/CFT Act. The following information has been published by DIA about the use of an NZDL:

Identification Standards Fit Information Assurance – The New Zealand Driver Licence can be used as evidence of the accuracy of information on the card, to varying levels of assurance.

Binding Assurance – The information on the card has been bound to the individual at a minimum of BA3.

Authentication Assurance – The New Zealand Driver Licence could qualify as an AA3 level authenticator, when presented in-person.

It is therefore our opinion that the documents specified in the IVCOP are restrictive without any apparent legal basis. They put unacceptable restrictions on reporting entities to decide which source they may use to verify the name or date of birth of a customer.

For example, a reporting entity could decide to use a document issued by a person's school, university or medical services provider that includes their full name and date of birth. We understand that these records are based on information about the person's full name and date of birth held in government databases.

A code of practice should not amend legislation or impose compliance obligations not specified under the Act.

We have received pursuant to an Official Information Act (**OIA**) request, a copy of a communication from the Director of DIA's AML/CFT group in which he tells staff of other AML/CFT Supervisors that DIA wishes *to make the IVCOP a gold standard*.

Information released to us under the OIA shows that the supervisors and MoJ have not conducted a cost benefit analysis of the IVCOP. However, the Cabinet Paper on the IVCOP states that it will "Minimise the regulatory burden, the impact on the public and compliance costs of the Act". From our interaction with our clients, it is abundantly clear that the IVCOP exponentially increases compliance costs, which are passed on to the public.

Further, it is counter-intuitive that a code of practice that is put in place to minimise regulatory burden requires two explanatory notes to explain measures that supposedly simplify the legislation.

The IVCOP should list the types of entities that may be considered reliable and independent. No further assistance would be required. For instance, a New Zealand government department should not be considered unreliable or conflicted.

We submit that:

- **A code of practice must be approved by the Minister of Justice**
- **A cost benefit analysis must be completed before a code of practice is put in place**
- **A code of practice must not alter the AML/CFT Act obligations to which it refers**
- **A code of practice must be voluntary but continue to provide a safe harbour if reporting entities have shown that they comply with it. The phrase 'equally effective means' should be removed from the legislation, along with the need to inform the supervisor of the reporting entity's decision not to rely on a code of practice. This phrase has been misused by supervisors to require reporting entities to adopt the IVCOP instead of following the requirements of s 13 of the AML/CFT Act by other means.**
- **An explanatory note to a code of practice should follow the same process as is required to put in place or amend a code of practice, if the note does more than provide an explanation.**

Consultation questions: AML/CFT Rules

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?

Our observation and submission

We have regulations that are made under the AML/CFT Act. Australia has rules. Compliance requirements under Australia's Act are similar but different to New Zealand's Act requirements.

In New Zealand regulations specify and/or add context to the obligations under the principal legislation. There does not seem to be any reason to use a separate mechanism to add context to obligations under the AML/CFT Act than for any other New Zealand legislation.

We submit that the current method of using regulations to add context to legislative obligations is working well. There are established processes in place to pass regulations. There does not seem to be any need for the government to adopt a separate process for the AML/CFT Act.

Consultation questions: Direct data access to FIU information for other agencies

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?

Our observations and submission

The FIU is provided information by reporting entities under suspicious activity reporting (**SAR**) on a mere suspicion of criminal activity, rather than on reasonable grounds. The requirement to report arises when, on the information available, a reasonable person would form a suspicion. The test does not require the reporting entity to consider whether reasonable grounds to conclude that an unlawful activity, relevant to one of the listed unlawful activities, has in fact occurred.

Further, as reflected in FAFTs 2021 review, FIU must upgrade its analytical tools to better use the financial intelligence to detect criminal activity by persons who are not already of interest to law enforcement, and to take advantage of reports on international funds transfers and large cash transactions. To collect but not use the information provided amounts to an interference with the private information of the public without reasonable justification.

We recommend that the Act should be amended requiring the FIU to delete all information that is provided by reporting entities that is not used to prepare actionable intelligence reports in a 5-year period from the date of the SAR or Prescribed Transaction Report (**PTR**) (consistent with other record keeping obligations under the AML/CFT Act), as an exception to the requirement to keep records under the Public Records Act.

Other law enforcement agencies should be permitted only to receive personal information about the public sent to the FIU by reporting entities through the mechanism of an intelligence report.

FIU already shares intelligence it collects with other law enforcement agencies under other enactments.

We submit that direct data access to information provided to the Police through an SAR or PTR should not be provided, as it will represent a violation of the public's right to privacy.

Consultation questions: Direct data access to FIU information for other agencies

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?

Our observations and submissions

Reports published by the FIU demonstrate that they provide intelligence reports to concerned law enforcement agencies. IRD is a recipient of intelligence reports prepared by the FIU.

Any data-matching proposals under the AML/CFT Act must be submitted to the Privacy Commissioner for review and feedback.

We submit that no additional powers be provided to the FIU to share data about the public.

Consultation questions: Registration for all reporting entities

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?

Our observations and comments

The government already requires financial institutions to register on the FSPR, or with professional bodies maintaining the registration and oversight of the non-financial designated businesses. Any additional registration is a duplication of effort and costs.

We submit that there should be no further registration regime introduced in New Zealand.

Consultation questions: AML/CFT licensing for some reporting entities

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?

Our observations and comments

The New Zealand economy is supported by small and medium sized businesses. It is known as one of the easiest countries in the world to conduct business. A licensing regime will create a barrier to entry into the market for both domestic and international entrepreneurs.

As stated above, without a regulatory impact statement on what the costs and possible unintended consequences of a licensing regime, submissions on this proposal are difficult to advance.

We submit that there should be no additional licencing requirements on reporting entities to enable them to provide services that are captured activities. The Ministry of Justice (**MOJ**) should be mindful that many of the services that are captured activities under the AML/CFT Act are classified as essential services. Putting additional restrictions on the public to launch and sustain a business that provides essential services to the public will cause more harm than good. It could also result in closure of small businesses that provide essential services to vulnerable communities.

Part 2 Scope of the AML/CFT Act

2.1 Challenges with existing terminology

Consultation questions - ordinary course of business

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 DFNBPs, 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?

Our observations and submission - ordinary course of business

The supervisors' guidance on how to determine the 'ordinary course of business' is well established. Reporting entities have not expressed any difficulties in exercising judgment when considering whether an activity is within the definition of 'ordinary course of business'.

We submit that no change is required to the use of the term and it provides appropriate relief to businesses that only rarely conduct captured activities.

Consultation questions - captured activities

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?

Our observations and submission - captured activities

The Act targets businesses conducting captured activities in the ordinary course of business. The supervised population is known and disclosed to supervisors because most activities must be conducted by licenced or certified businesses, I.e. licensed or certified by The Real Estate Authority (**REA**) (real estate agents), the NZ Law

Society (**NZLS**) (lawyers and conveyancers), the Chartered Accountants Australia & New Zealand (**CAANZ**) (accountants), the Financial Markets Authority (**FMA**) (financial market service providers), the Reserve Bank of New Zealand (**RBNZ**) (bank, insurers and non-bank deposit takers) and/or the Commerce Commission (consumer lenders).

Unlicensed or uncertified entities, such as trust and company service providers that aren't licensed statutory supervisors, creditors under non-consumer credit contracts and those operating a money or value transfer service must be registered on the Financial Service Providers Register (**FSPR**).

All reporting entities must be recorded on the FSPR by disclosing the financial service they provide as stipulated in 7A(1)(e) of the Financial Service Providers (Registration and Dispute Resolution) Act (**FSP Act**) but subject to s 7, which excludes FSP registration of businesses licensed or enrolled with REA, NZLS or CAANZ. To make it clear that real estate agents, lawyers, conveyancers and accountants must be registered on the FSPR and comply with AML/CFT measures if they are providing financial services to clients, the s 7 exclusion requires amendment so that only businesses licensed by REA, NZLS or CAANZ and **not** providing financial services to their clients in the ordinary course of business are excluded from the need to register on the FSPR.

We submit that entities that undertake captured activities as hybrid businesses must comply with AML/CFT measures. Only a minor amendment is needed to the FSP Act to achieve the change needed. Further, duplication of work is minimal for hybrid businesses and an exemption from duplication does not appear to be required.

Consultation question - regulations for captured activities

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?

Our observations and submission - regulations for captured activities

For the reasons above, we submit that issuing regulations to clarify the Act in this respect is unnecessary.

Consultation questions - 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?

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?

Our observations and submission - managing client funds

Overlap of captured activities occurs frequently, but occasionally financial institutions and DNFBP that are not otherwise captured by other activities are captured by the 'managing client funds' activity.

Regardless of a reporting entity being captured by multiple activities listed in the definitions, there are only a few obligations that are duplicated. For example, account monitoring will be required for all accounts, regardless that one client has an account for a real estate transaction, and another for the settlement of a trust. Customer due diligence does not need to be conducted twice for the same client regardless of the different activities conducted. There seems to be little duplication.

Professional fees are payment by or on behalf of the customer for the scope of service agreed to be provided by the reporting entity and should include disbursements required to be paid when carrying out the scope of services, such as third-party fees.

We submit that no changes are required to 'managing client funds', 'professional fees' should be defined as payment by or on behalf of the customer for the scope of service agreed to be provided by the reporting entity and includes disbursements required to carry out the scope of services, such as third-party fees.

Consultation questions - alignment with FSP 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?

Our observations and submission - Alignment with FSP Act

An example of how the AML/CFT Act and the FSP Act can align better is set out in the submission to questions 2.4 and 2.5 above, to make it clear that captured activities require AML/CFT measures regardless of whether the reporting entity regards itself as a financial institution or a DNFBP. Further alignment is required for the definitions of 'financial services' in the FSP Act and 'financial institution' for the

AML/CFT Act to ensure visibility of the full population of financial institutions can be achieved by the mandatory requirement for registration on the FSPR.

We submit that alignment between the FSP Act and AML/CFT Act is required.

2.2 Potential new activities

Consultation questions - VASP

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?

Our observations and submission - VASP

Wallet providers are caught in the definition of financial institution under the category described as '*accepting deposits* or other repayable funds *from the public*'. Crypto currencies are deposited into a virtual providers wallet for safekeeping and they are payable to the customer on request. Deposits include both fungible and non-fungible products.

We submit that the definition of financial institution is sufficiently wide to capture virtual wallet providers' and other VASP activities.

Consultation questions - Charities

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?

Our observations and submission -Charities

Only charities that operate in overseas jurisdictions should be subject to AML/CFT measures. To impose measures on charities operating locally would create disproportionate costs of compliance relative to the risks of ML/TF. For example, many charities are associated with schools in NZ, these are regulated by Charity Services, part of DIA, and have tax exemption and donee status granted by Inland Revenue. There is usually only a discrete pool of beneficiaries (the school and its

population) that may benefit from the charity under the Deed of Trust that establishes the school charity. Further the school itself is regulated by the Ministry of Education. Charities of this kind present no risk of TF and should not be put to the cost of compliance with the Act.

We submit that only NZ charities that operate overseas should be subject to the AML/CFT Act.

2.5 Territorial Scope

Consultation questions - Territorial scope

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?

Our observations and submission - Territorial scope

The territorial scope of the AML/CFT Act should align, as far as relevant, with the territorial scope provisions in s 7A of the FSP Act, but exclude the FSP Act's threshold provisions set out in regulations, which could encourage structuring to avoid meeting threshold limits.

We submit that territorial scope of the AML/CFT Act should align with the FSP Act but will also need to stipulate thresholds will not apply for reporting entities.

Part 3 Consultation questions: Agency supervision model

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?

Our observations and submission

The three supervisors' model does not work well. We have observed several inconsistencies in the way three AML/CFT Supervisor operate. An example is recent Sector Risk Assessment published by FMA that recognises that it supervises only a small number of VASPs reporting entities, the rest of the sector are supervised by DIA. Having a sector split between supervisors depending on the reporting entity's business model is inefficient, requires the duplication of skills in the supervisors and has led to inconsistencies in the application of the legislation. Further the FMA's sector risk assessment simply relies on the DIA's sector risk assessment for VASPs

and so the FMA has abdicated its responsibility for assessing risk in a sector to the DIA without commenting on the adequacy of that assessment for its own population.

FMA has informed us pursuant to an OIA request that guidance issued by AML/CFT supervisors is non-binding, non-mandatory and not enforceable. DIA has informed a reporting entity known to the authors, who wishes to remain anonymous, that DIA regulates to its guidelines.

We submit that New Zealand should have a single entity under the MOJ that is responsible for AML/CFT Act supervision.

Consultation questions: Mechanisms for ensuring consistency

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?

Our observations and submission

The Act appropriately ensures consistency. However, the three supervisors do not consistently apply the same legislation.

An example of this is the obligation to file a prescribed transaction report for international wire transfers of $1000 and over.

The policy intent of this obligation is that the reporting entity that first handles the funds entering New Zealand (first receiver) and the reporting entity that last handles the funds before they leave New Zealand (final sender) should report the transaction.

The Cabinet Paper about this amendment (that was released under an OIA request) indicates that it was anticipated that this obligation would affect banks and money remittance companies who make international wire transfers outside the mainstream banking system.

The MOJ has informed us pursuant to a request made under the OIA that there has been no change in the policy intent of this requirement.

FMA has confirmed that if a reporting entity conducts a wire transfer through a bank, then the bank will submit the PTR. This aligns with the policy intent of the legislation as explained to Cabinet.

DIA has informed DNFBPs, such as law and accounting firms, that they must file a PTR even though an international wire transfer is conducted through a bank.

Our experience working with several of our clients is that DIA requires all reporting entities that are part of an international wire transfer, even if they are not the first receiver or final sender institution, must file PTRs. FMA does not require this.

There is a clear differentiation in compliance costs for FMA and DIA reporting entities.

We brought this inconsistency to the attention of the MOJ. The MOJ should co-ordinate and be responsible for ensuring consistent supervision across the three AML/CFT supervisors did nothing to correct this inconsistency.

We submit that there should be one AML/CFT Act supervisor, this is because the three supervisors model has resulted in inconsistent supervision across the private sector, resulting in inconsistent compliance costs.

Consultation questions-Powers and functions

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

Our observations and submissions

The functions of the supervisors are appropriate. However, the powers provided under s 132(1) of the AML/CFT Act are broad and subject to abuse without appropriate controls or limits.

We have seen several instances of abuse of power by supervisors. These are around:

- Requiring reporting entities to amend their risk assessment and/or programme where the supervisors are unfamiliar with the risks posed in the subject businesses;
- Requiring compliance actions by a reporting entity not available under the Act;
- Targeting reporting entities with more intensive supervision when they choose to not adopt the IVCOP.

We submit that the powers provided to supervisors under s 132 are too broad. There is currently no ability to independently review the supervisors' conduct without commencing expensive judicial review proceedings. An office of an independent reviewer should be established for this function.

Consultation questions – Remote inspections

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?

Our observations and submissions

Powers under s 133 are broad and could be used to violate a reporting entity's rights guaranteed under s 21 of the Bill of Rights Act.

We have personal experience of a supervisor conducting inspection of documents during site visits even though s 133 permits the asking of questions, not the inspection or copying of documents without providing reasonable notice (s 132(2)(a)).

In our experience, DIA officials have, during a site visit of a Chinese owned reporting entity, enquired whether the reporting entity's employees have a right to work in New Zealand. These questions appear irrelevant to the obligations under the Act.

We submit that the powers available to supervisors under the Act must be subject to the rights provided to the public in the NZBOR and the Human Rights Act 1993.

Consultation questions – Independent auditors

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?

Our observations and submission

An audit under s 59 or s 59A must be carried out by an independent person, appointed by the reporting entity, who is appropriately qualified to conduct the audit.

The Act currently provides the reporting entity the discretion of deciding on an appropriate auditor.

To our experience most audits are currently being conducted by people who have received AML/CFT related training that is not specific to New Zealand's Act.

Currently, price is the main factor that reporting entities appear to be using to select an auditor. Supervisors accept poor audit reports and do not ask reporting entities to demonstrate to them how they have ensured that the auditor was appropriately qualified to conduct the audit.

Requiring a specific number of years working with the AML/CFT Act or any financial audit qualifications could exponentially increase audit costs. Businesses who rely on

the recommendations and observations of their auditor to help them meet their obligations should have a defence of *reasonable reliance* introduced in the Act.

Some of the issues with regards to audits stem from different expectations from supervisors. During an auditor outreach, one official stated that he would like to see only an exceptions report. Other officials like to see more detailed audit reports.

We submit that

a) **Setting standards for audits akin to financial audits would make them prohibitively expensive for small reporting entities.**
b) **The Act should not be amended to include standards for audits.**
c) **The Act should be amended to replace the terms independent audit with independent review.**
d) **The format of the review conducted by an independent appropriately qualified person should be specified in Regulations.**
e) **Reporting entities who rely on the recommendations and observations of their auditor to help them meet their obligations should have a defence of *reasonable reliance* introduced in the Act.**

Consultation questions: Consultants

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?

Our observations and submission

We submit that the Act is just one piece of legislation that reporting entities must comply with. The government must not create barriers to firms for selecting who they wish to seek assistance from. Reporting entities can proceed against a consultant for incompetent advice under breach of contract and/or negligence proceedings. Standards will vary depending on the size, risks and resources of a reporting entity's business. One size does not fit all.

We also submit that MOJ must make it clear to supervisors that they can only *allege a breach* of the Act, only the Courts can decide if the Act has been breached.

Consultation questions: Comprehensiveness of penalty regime

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?

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?

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?

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?

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?

Our observations and submission

AML/CFT supervisors cannot decide if a reporting entity's conduct has breached legislative provisions. In New Zealand, only the courts can decide if a legislation has been breached.

The AML/CFT Act currently has sufficient penalties if the reporting entity is reckless in meeting its compliance obligations.

A lack of comprehensive documents or a failure to conduct CDD correctly or monitor customer accounts to detect anomalies by a reporting entity does not mean that ML/FT has occurred or that the conduct has resulted in harm to society.

If there has been no evidence that a reporting entity's actions have resulted in crime going undetected, why should the New Zealand government initiate proceedings against the reporting entity?

It also does not mean that the reporting entity has been complicit in the predicate criminal activities.

MoJ should take into consideration that in New Zealand it is not mandatory to report crime (other than that which involves harm to children) to law enforcement agencies.

The AML/CFT Act currently permits reporting entities to prepare their AML/CFT risk assessment and AML/CFT programme to the best of their knowledge. Supervisors with little knowledge of the business operations of a reporting entity should be required to provide evidence why the documents will result in ML/FT occurring undetected through a reporting entity before initiating court proceedings in respect of those documents.

The RBNZ is aware that Banks do not open accounts for certain businesses due to the bank's assessment that another reporting entity may not meet their own AML/CFT compliance obligations. This is denying businesses the ability to obtain essential banking services and places the Bank in the role of decision-maker of other reporting entities are compliant with their obligations under the Act.

We submit that:

- **AML/CFT supervisors must be prevented from warning a reporting entity that their conduct constitutes a breach of any provisions of the Act. Only the courts can decide if alleged conduct is a breach of the AML/CFT Act.**
- **Proceedings against a reporting entity for failure to meet AML/CFT Act obligations should be permissible only if it becomes evident that the conduct has resulted in measurable harm to the New Zealand public.**

Part 4 Preventative measures

Customer Due Diligence

Consultation questions - CDD

4.1 - 4.75 What challenges do you have with complying with your CDD, enhanced CDD and suspicious transaction obligations? [Various questions not repeated here]

Our observations and submission - difficulties with CDD

The obligations to conduct CDD and the requirement to obtain verification of the name and date of birth of each customer, or each person acting on behalf of a customer are in place to help the reporting entity understand who their customer is and the extent of the business relationship that the customer wants with the reporting entity.

Forcing reporting entities to speculate on which customers could conduct ML/FT (without any evidence of their actual involvement in these activities) is unlikely to make New Zealand a better, freer society. On the contrary, it creates an environment of distrust between the public and essential service providers within New Zealand.

The AML/CFT Act, and the way it is being implemented, has not enhanced the confidence of the public in the financial system. Entire financial sectors are denied access to banking services. The various public meetings conducted by DIA and RBNZ indicate that they are aware of this. So far, the government has taken no steps to rectify the situation.

The beneficial ownership guideline issued by the supervisors is confusing. Supervisors have included 'person on whose behalf a transaction is conducted' as a beneficial owner. This could effectively make a customers' customer the beneficial owner. Where does the chain of benefit stop?

These issues were raised when supervisors published the guideline. In response to the objection from reporting entities to supervisors' interpretations, MOJ passed the Licenced and Specified Managing Intermediaries class exemptions. The exemption does not address the underlying issue.

The interpretation of *beneficial ownership* continues to be a significant issue for reporting entities.

As we have mentioned earlier, the IVCOP increases compliance costs, and raises barriers to the public to access essential services, by stating that there are obligations to conduct identity verification in ways that are not stated in ss 13, 15, 16 of the AML/CFT Act.

Conducting CDD on customers as required under ss 13, 15 and 16 of the AML/CFT Act is simple, the IVCOP confuses and complicates the practice of identity verification.

Sections 15 and 16 of the AML/CFT Act requires a reporting entity to, amongst other things, obtain and verify a customer's address. Supervisors require reporting entities to obtain a customer's *residential address*. This is not a requirement under the Act.

An example of the supervisors acting to complicate a simple exercise of identity verification, was their guideline that an expired passport cannot be used to verify a person's full name and date of birth. Under an OIA request, the DIA has informed the submitters that when a passport expires the DIA does not become an unreliable entity for the purpose of s 13. A New Zealand passport is a travel document and cannot be used for international travel when it expires. However, the holder's name and date of birth do not change. The question then is, why is an expired passport used to verify a customer's full name and date of birth unacceptable. Requiring a

current passport to enter relationships with financial service providers is an unreasonable barrier, particularly to lower socio-economic groups. By DIA's own admission an expired passport is nevertheless a document issued by a reliable and independent source and therefore permissible under s 13 of the AML/CFT Act.

Further difficulties arise when reporting entities must comply with the explanatory note issued in July 2021 (**Explanatory Note**) in respect of Part 3 of IVCOP, in relation to electronic verification (**EV**). The Explanatory Note was published by the Supervisors without consultation.

The submitters OIA request for information made to MoJ about the consultation carried out by the supervisors requested the following information:

… 2. the consultation that the supervisors conducted with the Ministry of Justice with regards to the two Explanatory Notes to the Identity Verification Code of Practice 2013 that AML/CFT Supervisors published;

3.the Ministry of Justice's communications with AML/CFT/CFT Supervisors about the above-mentioned Explanatory notes. …

MoJ provided the following response:

The Ministry does not hold any material relating to the consultation on the explanatory notes to the Identity Verification Code of Practice 2013.

The Explanatory Notes amend the requirements for Electronic Identity Verification included in the IVCOP 2013. Information released to the submitters under the OIA request indicates that proper process was not followed to make the amendments.

The Explanatory Notes provides a monopoly for the DIA in respect of its EV solution, RealMe in respect of being regarded by the supervisors as the *only single independent electronic source that can verify an individual's identity to a high level of confidence*.

The RealMe EV product is expensive ($8 per verification) and an API to a reporting entities on-boarding system is only economic for larger financial institutions. This is because integration involves the secure linking to the RealMe service. This is enabled via RealMe's technical development integration team, which it does not charge for, but a reporting entity bears its own costs of integration.

However, in practice there have been instances where RealMe accounts have been misused, by the stealing or giving of passwords, to establish fraudulent accounts with reporting entities. Identity verification via RealMe is just as susceptible to fraud as any other identity fraud, e.g. For instance, using a fake or fraudulent document, scanned to a reporting entity for matching against the NZDL database. Accordingly, the status provided to RealMe is artificial and requires review by MOJ.

Additionally, since DIA is effectively in trade with regards to the sale of its RealMe service. It must not be permitted to use its position as an AML/CFT supervisor to artificially create an anti-competitive environment in which other Identity

Verification Services (**IVS**) cannot compete with DIA for the provision of identity verification services. There is a thriving industry of IVS providers that have had their businesses effected by the change to the IVCOP via the Explanatory Note. There may be Commerce Act implications if DIA uses its power to create an environment where its competitors are unable to operate.

Further difficulties arise where customers provide foreign identity documents that are difficult to verify as correct against overseas government databases, as required by the Explanatory Note. The purpose of the Act is not to detect fraud. In all cases, the reporting entity should be entitled to assume that identity documents presented by a customer either in person or electronically are legitimate and true, unless the reporting entity has reasonable grounds to suspect that the documents are not.

Additionally, the Contracts and Commercial Law Act 2017 permits businesses to accept documents sent to them electronically. The IVCOP and its Explanatory Note should not restrict reporting entities deciding to accept IV documents electronically if there are no grounds to suspect that the customer's documents are fraudulent.

We note that the consultation document mentions that the AML/CFT Act requires a reporting entity to obtain and verify the source of funds or source of wealth of a customer.

That is incorrect. The obligations under s 23(1) are as follows:

23Enhanced customer due diligence: identity requirements

(1) A reporting entity must, in relation to a person referred to in section 11(1), obtain the information required under section 15 and the following additional information:

(a) information relating to the source of **the** funds or **the** wealth of the customer; and

(b) the additional information referred to in subsection (2) and any additional information prescribed by regulations.

We observe that the provisions under s 23(1) appears to have been misinterpreted by MoJ in the consultation document.

We also observe that the AML/CFT supervisors Enhanced CDD guidelines interchangeably uses source of funds and source of the funds.

There is a significant difference between source of **the** funds or **the** wealth that could be used by a customer in a business relationship or occasional transaction.

The requirements for reporting entities to monitor their customers' accounts to determine that the activity aligns with expectations is adequate in the current legislation.

The AML/CFT supervisors should not be permitted to pass a code of practice (together with explanatory notes) that are broader than the existing

obligations under the AML/CFT Act, particularly if those codes and explanatory notes are not widely consulted on.

We submit that the IVCOP should be reviewed by MOJ (including by public consultation) for the following reasons:

- **It significantly increases compliance costs, without any calculated corresponding benefits;**
- **It prevents the use of documents to verify an individual's full name and date of birth that meet the basis for verification of identity specified under section 13 of the AML/CFT Act;**
- **It forces face-to-face contact to verify a person's full name and date of birth and promotes an antiquated method of doing business;**
- **It does not take into consideration the permissibility of documents being transmitted electronically, as permitted in the Contracts and Commercial Law Act 2017;**
- **It permits the use of bank cards to verify the information on an NZDL even though they do not include the identical information and, it puts card holders at risk of breaching the terms and conditions under which the card was issued.**

We submit that a IVCOP should be limited to helping reporting entities determine what type of entity could be considered as reliable and independent.

The IVCOP should not include a statement of practice that could:

- **Be more complex and/or expensive to follow than s 13 of the AML/CFT Act.**
- **Require expensive electronic means to verify the authenticity of documents if identity documents are sent electronically. The government has enacted legislation that permits business to accept at face value documents sent electronically to them. The AML/CFT Act is not anti-fraud legislation.**
- **Unreasonably affect the right to privacy of the public.**

We surmise that the RealMe EV solution provides no more surety of the identity of the person tendering the RealMe account, than any other photographic identity document. Therefore, the Explanatory Note should be reviewed to consider whether:

(1) it amends part 3 of the IVCOP;

(2) due process required under the AML/CFT Act for amending a code of practice was followed before the Explanatory Note was published;

(3) the *high-degree of confidence* status declared by the supervisors to be held by RealMe is in fact the case.

We submit that if it is found that the Explanatory Note amends the IVCOP it should be withdrawn as it has not followed due process required under the AML/CFT Act to amend a code of practice.

We submit that there is a significant difference between source of funds or source of wealth and source of the funds or the wealth. AML/CFT supervisors must not be permitted to issue guidelines that amend core obligations under the AML/CFT Act.

Consultation questions – Record keeping

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?

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?

Our observations and submission - record keeping

Generally, reporting entities have little issue complying with record keeping obligations.

Section 50 of the AML/CFT Act includes the following obligations:

50 Obligation to keep identity and verification records
(1) In respect of each case in which a reporting entity is required, under subpart 1 of this Part, to identify and verify the identity of a person, the reporting entity must keep those records that are reasonably necessary to enable the nature of the evidence used for the purposes of that identification and verification to be **readily identified** at any time.
(2) Without limiting subsection (1), those records **may** comprise—
(a) a copy of the evidence so used; or
(b) if it is not practicable to retain that evidence, **any information as is reasonably necessary to enable that evidence to be obtained.**

It is clear that it is not mandatory under the AML/CFT Act to keep a copy of the document that was used to verify the person's full name and date of birth or address. Additionally, when submitting a SAR to the police, the reporting entity is not required to upload the documents that were relied on to verify the person's full name date of birth and address.

We have encountered a supervisor insisting that a reporting entity keep a copy of the customer's identity document.

Forcing reporting entities to keep a copy of the document that was used to verify a person's full name and date of birth could expose the public to identity theft if the reporting entity was subject to a data breach either electronic, or physical.

Where issues of records become difficult is when reconstructing transactions requested under the information gathering power of the supervisors at s 132 of the Act. Supervisors must be cognisant of the need to provide reasonable notice when requesting documents and information under that provision. The need to provide notice to a reporting entity is not lost purely because the supervisor is requesting information in documents during an inspection under s 133 of the Act. Section 133 does not permit the Supervisor to conduct a search. Section 133(2) specifies that a supervisor may require a reporting entity to answer questions relating to its records and documents and to provide any other information that the supervisor may reasonably require for the purpose of the inspection. It does not allow the supervisor to require the delivery of a reporting entities documents themselves.

Section 13 demonstrates that documents, data or information are treated as separate constructs under the AML/CFT Act. If Parliament had intended for supervisors to have the powers to require documents to be submitted during a site visit, it would have been specified under s 133 of the Act.

Our experience is that supervisors have expected immediate delivery of documents during an inspection based on the requirement in s 49 that every transaction must be readily reconstructed at any time. Had immediate delivery been contemplated by the Legislature then the requirement for notice under s 132 would not exist. Further, demands for immediate delivery is likely to be a breach of s 21 of the NZBORA as an unreasonable search and seizure.

We observe that the documents that are required are not necessary to prevent any immediate harm to any individual, institution or the NZ public in general. We also observe that the NZ government requires 20 working days at a minimum to respond to a request for documents made under the Official Information Act. The government must not impose restrictions on the public that it does not impose on itself under similar circumstances.

We submit that the supervisors must be mindful that delivery of documentary information can be required only on reasonable notice to the reporting entity, and that the expectation of immediate delivery may be a breach of the NZBORA.

We submit that MoJ must clarify the requirement of se 50 of the Act to supervisors. Supervisors should not be permitted to insist that reporting entities keep a copy of the document that their customers provide to verify their full name and date of birth, when the Act does not stipulate that.

Consultation questions – Politically exposed persons

4.79 -4.99 Various questions posed about PEP requirements under the Act?

Our observations and submission – Politically Exposed Persons

There are currently no publicly available search engines that will enable a reporting entity to be able to identify a PEP to a high degree of accuracy. Section 5 of the Act provides that a PEP includes:

… any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or **any other close relationship**, with a person referred to in paragraph (a); or any individual who has sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph (a).

There are currently no mechanisms available to accurately assess the probability of a PEP resident in New Zealand being involved in criminal activity. On what basis does MOJ expect reporting entities to determine if a PEP could be involved in ML/FT?

Requiring reporting entities to identify certain political entities, government officials, their immediate family members and close associates and then raise barriers to these individuals accessing essential services is unreasonable.

We submit that the compliance obligations placed on reporting entities of the steps that they must follow before they can offer their services to a PEP must not violate the rights guaranteed to the PEP under s 17 of the NZBORA and The International Covenant on Economic, Social and Cultural Rights ratified by New Zealand on 28 December 1978.

Consultation Questions – Targeted Financial Sanctions

4.103-4.119 Various questions regarding the implementation of Targeted Financial Sanction (**TFS**) obligations under the AML/CFT Act.

Our observations and submission – TFS

TSF are enacted under separate legislation. There are prohibitions from engaging with entities or individuals who are subject to such TFS.

TFS may not be put in place to prevent money laundering or financing of terrorism or the predicate offending that generates illegal funds. There may be other political considerations for the imposition of TFS.

The government will know the details of a person or entity who is subject to TFS. It will have the means to directly monitor their activity without forcing the private sector to be involved in this aspect of its function.

The private sector already pays the government through its taxes to meet its international obligations, including those to the UN.

We submit that the government should use its existing law enforcement resources to enforce TFS and not impose additional compliance costs on reporting entities to help it to implement TFS.

[See also our observations in respect of TFS at 1.4, 1.6 and 1.34]

Consultation Questions - Ensuring agents comply with AML/CFT obligations

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

Our observations and submission- Ensuring agents comply with AML/CFT obligations

The consultation document states:

Under the general law of agency, the principal (i.e., the MVTS provider) is bound by the actions of their agents.

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 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.

Section 57(1) (k) currently requires a reporting entity's AML/CFT programme to include adequate and effective policies, procedures and controls for relying on third parties to conduct CDD on their behalf.

We submit that ever since the AML/CFT Act, MVT sector has been subject to denial of banking services. This has had a negative impact on this sector. RBNZ's governor has publicly stated that denial of banking services is detrimental to the economies of small Pacific Island countries.

Therefore, before the proposed regulations are considered it is essential that there is extensive consultation with the MVT sector on the issue.

We submit that the suggested regulations should be passed only if MoJ has conducted impact analysis that establishes that such regulations:

- **do not result in additional AML/CFT Act compliance costs to MVT;**
- **will not raise additional barriers in MVTs having access to banking services**
- **are essential to reducing harm to society from crime and/or terrorism.**

Consultation Questions – Prescribed transaction reports (PTR)

4.156 Are the prescribed transaction reporting requirements clear, fit-for-

purpose, and relevant? If not, what improvements or changes do weneed to make?

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

Our observations and submission - PTR

Information published by FMA on who is responsible for filing PTRs aligns with the policy intent included in the Cabinet Paper on PTRs. It sets the responsibility for filing PTRs on Banks as they will, under most circumstances, be the last institution to handle the funds before they exit the country or the first to handle the funds when entering the country.

We have encountered DIA insisting the reporting entities it supervises must submit PTRs even though the international wire transfers are conducted through a Bank. This results in unnecessary reporting duplication.

We submit that the DIA and FMA must issue consistent PTR guidance, which does not impose disparate compliance costs for reporting entities supervised by supervisors.

Consultation questions - Internal policies, procedures, and controls

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

Our observation and submission

The minimum requirements set out under s 57(1) are not well articulated.

The subsections are repetitive. For example, s 57(1)(c) is about CDD, ongoing CDD, and account monitoring. Section 57(1)(g) is about written findings that would be better included under account monitoring. Section 57(1)(j) is about enhanced CDD and simplified CDD when the obligations are prescriptive and are covered under s 57(1)(c). Section 57(1)(k) is about reliance on third parties, which is also a factor covered under s 57(1)(c). The requirements of s 57(1)(f) are superfluous, as the entire programme is the reporting entity's risk mitigation instrument.

Section 57(1)(l) requires policies, procedures and controls for compliance with the programme and training in the programme. Compliance with the programme is covered by the controls for each of the preceding sections. Training in the programme will be covered under the training section of the programme.

Section 57(1) presumes that all the elements under it are equally applicable to all reporting entities. This is not the case. A reporting entity that is a sole trader operating a non-bank, non-deposit-taking lender that lends only to persons

resident in New Zealand, will not require policies, procedures and controls to keep written findings about overseas transactions specified under section 57(1)(h). It will also not require policies, procedures and controls for staff vetting.

We have encountered supervisors telling reporting entities to include policies, procedures and controls in their programme for vetting regardless that they do not employ staff and the firm is operated by its owner. We have also encountered a supervisor telling a reporting entity that they were non-compliant with regards to vetting, because vetting was not conducted on the managing director who is also the firm's beneficial owner. The official was effectively demanding that the business owner must vet themselves. How will such conduct by staff of supervisors increase the public's confidence in the payment system or deter and detect ML/FT?

We submit that the obligations in s 57 of the Act should be reviewed to better articulate the minimum requirements of a programme. However, if a subsection is not applicable to a reporting entity, then the entity is not required to provide for it, other than a dismissal of its applicability to its business.

We submit that supervisors must not be permitted to direct a reporting entity to amend its programme. Such powers should only be available to the courts. The Act enables supervisors to approach the courts to direct reporting entities to provide a binding undertaking to amend conduct.

We further submit that if supervisors wish to recommend to the reporting entity that it amends its risk assessment or programme the supervisor must be directed to provide evidence to the reporting entity that without the amendments, the risk assessment and/or programme will result in ML/FT occurring undetected through the reporting entity.

Consultation questions – Review and audit requirement

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 isrequired?

4.193 Should legislation state that the purpose of independent audits is totest 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 isuseful for businesses without imposing unnecessary compliance costs?

Our observations and submission – Review and audit

The Act is a set of policies, procedures and controls to enable a reporting entity to meet legislative requirements.

Requiring the AML/CFT programme to be reviewed without a change in legislation or the reporting entity's operations is an unnecessary exercise.

Section 59 specifies that a risk assessment and programme must be audited. The Act sets limitations on the audit of a risk assessment.

Section 57 requires an AML/CFT programme to include adequate and effective procedures, policies, and controls for certain minimum requirements.

The Act does not interpret what is required for the policies, procedures and controls to be adequate and effective, nor does it include measures that auditors or supervisors use to form an opinion on whether a reporting entity's policies, procedures and controls are adequate and effective.

Independent review about a firm meeting its compliance obligations is necessary to give assurance to the reporting entity. The recent regulatory amendment to require this independent assurance to be obtained every three years instead of the previous two years.

This could indicate to reporting entities that the government does not consider it important for them to obtain an independent opinion about the effectiveness of their compliance regime.

We observe that some auditors have no training on the New Zealand Act. Their training is limited to training provided by overseas based organisations with little or no training provided on how a reporting entity should meet their obligations under the Act.

We submit that the purpose of an audit of a reporting entity's AML/CFT risk assessment and AML/CFT programme is to provide it assurance about their implementation. MoJ should review whether seeking independent assurance every three years is sufficient.

We submit that MoJ consider regulating the format of an audit. Such a format will ensure a level playing field for reporting entities with regards to audits. It will also provide supervisors a standard set of tests that must be carried out to determine if a reporting entity has effectively met its compliance obligations.

In the absence of mandatory benchmarks for adequacy and effectiveness of the policies, procedures and controls of a programme, supervisors and auditors cannot form uniform and informed opinions as to whether the policies, procedures and controls are adequate and effective.

Consultation questions – Higher risk countries

4.195. How can we better enable businesses to understand and mitigate therisk 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?

Our observations and submission – Higher Risk countries

The Act does not refer to higher risk countries. The New Zealand government does not have a list of 'higher risk countries' that reporting entities can rely on.

The Act does not currently require a reporting entity to assess whether a country it might have customers, or business relationships in, or accept transactions from, is a high-risk country.

We have encountered DIA staff asking reporting entities to treat China as a high-risk country. China has not been identified by FATF as being a country with insufficient, or no ML/FT systems or measures. Pursuant to an OIA request the Ministry of Foreign Affairs and Trade has provided information that suggests that New Zealand considers China to be an important trading partner.

We note that RBNZs' guidelines suggest that a country that has a fundamental problem with organised crime could be a high-risk country. If that is so, then New Zealand, with a serious problem of trade in illicit drugs by organised criminals, is a high-risk country. Therefore, all transactions in or out of New Zealand must be subject to additional scrutiny by other countries with which New Zealand's financial institutions transact.

Only FATF's mutual evaluations are accepted as a benchmark for determining a country's adherence to FATF's 40 recommendations.

We submit that the Act should specify that the only mutual evaluation assessments conducted by FATF should be used to determine if a country has sufficient or no AML/CFT systems or measures. This information is publicly available at no cost.

We submit that AML/CFT supervisors should not be permitted to ask reporting entities to make assumptions with regards to its dealings with individuals or entities based overseas unless they are established on FAFT's recommendations identifying the countries as having insufficient or no ML/FT systems or measures.

Consultation questions Suspicious activity reporting

4.203. How can we improve the quality of reports received by the FIU andavoid low-quality, defensive reporting?

4.204. What barriers might you have to providing high quality reporting to theFIU?

4.205. Should the threshold for reporting be amended to not capture low leveloffending?

4.206. How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?

4.207. What barriers might you have to providing high quality reporting to the FIU?

4.208. Should the threshold for reporting be amended to not capture low level offending?

4.209. If a SAR is required, should it be explicitly stated that it must be submitted in any jurisdiction where it is relevant?

Our observations and submission

Pursuant to an OIA request, the previous Minister of Justice has informed that the New Zealand government has no plans to make it mandatory to report the predicate crime that might be involved in generating the illegal funds requiring laundering.

Predicate crimes, such as drug dealing and human trafficking, cause significant harm to society.

It is arguable that the act of laundering causes less harm than the predicate offending (although it is accepted that the funds may be used to finance further offending). It is manifestly unfair to impose penalties as high as $4m on reporting entities for not reporting the suspicion of money laundering, when there is no obligation on New Zealanders to report far more heinous crimes.

The high fines for non-reporting of suspicious activity could be a contributing factor in the defensive reporting mentioned in the consultation document. Forcing a reporting entity to secretly report activity of their customers, under threat of high fines, to the police merely on suspicion violates the rights to privacy of the public and the right to unreasonable search and seizure. The police have sufficient powers under existing laws to obtain information from the public.

Care must also be shown to the threat of retribution that a reporting entity could face from organised crime if they are forced to report their activity to the police.

We understand that FATF's recommendations do not require countries to criminalise the non-reporting of SAR to the extent that they are currently criminalised under the AML/CFT Act.

We submit that to reduce the defensive reporting that is mentioned in the consultation document, measures other than large penalties should be considered.

We also submit that consideration must be given to providing protection to reporting entities from physical violence that they might be subject to by a customer whose activity was reported to the police.

We further submit that consideration must be given to specifying through regulations, the process that a reporting entity should follow to determine that there are reasonable grounds for forming a suspicion that an activity is linked to crime or terrorism.

Part 6 Minor Changes

Definitions, information sharing, SARs/PTRs, offenses and penalties and preventative measures

Our observations and submission

The *minor changes* listed in the chart at the end of the consultation document are not minor. The body of this submission has covered some of the issues raised in the chart.

For example, the proposal to widen the information sharing powers significantly, including the ability to instigate investigations by supervisors under a request from an overseas government. As stated in the body of this submission, the police have other legislation that allows it to respond to overseas requests. Unless there are deficiencies in that legislation, the AML/CFT Act should not be broadened. Further, any proposed increase in government/supervisor/FIU information sharing powers should be submitted to the Privacy Commissioner for review.

We have also submitted above that reasonable notice is required to be given by the supervisors before requiring the delivery of documents or information by a reporting entity. For that reason, the amendments proposed to s 52 to clarify that records must be made available immediately (e.g. upon request from a supervisor) is improper given the requirement for reasonable notice to be provided under s 132(2)(a) of the Act.

The debt collection services exemption amendment is puzzling. The amendment suggests that the definition of debt collection services should be amended to state that it only relates to the collection of unpaid debt, rather than the collection of any funds owed by one person to another. Funds owed by one person to another is 'unpaid debt'. What is required for a debt to be owed are parties in a debtor/creditor relationship, regardless of whether an agent is appointed by the creditor to collect the debt.

We submit that the 'minor changes' referred to in Part 6 of the consultation document should not be enacted without considering the pertinent submissions that we have made in this document.