aml

From: [redacted]@nikkoam.com>
Sent: Thursday, 16 December 2021 2:41 pm
To: aml
Subject: RE: aml/cft Act review consultation - Request for extension on behalf of BIG group
Attachments: BIG-submission-MoJ-AMLCFT-2021-12.pdf

Good afternoon Nick

Please find attached a submission on behalf of the Boutique Investment Group (BIG)

I hope that you have a relaxing Christmas break.

Kind regards

[redacted]

From: [redacted]
Sent: Wednesday, 1 December 2021 10:30 AM
To: aml <aml@justice.govt.nz>
Subject: RE: aml/cft Act review consultation - Request for extension on behalf of BIG group

Thanks Nick

We shall do our best

Kind regards

[redacted]

From: aml <aml@justice.govt.nz>
Sent: Wednesday, 1 December 2021 10:26 AM
To: [redacted]@nikkoam.com>
Subject: RE: aml/cft Act review consultation - Request for extension on behalf of BIG group

Kia ora [redacted],

Many thanks for your email. If it is at all possible to get the submission in by the 10th that would be ideal from our perspective – but if you would prefer the 17th we can also accommodate that. Most businesses/groups have sought and been given a 1 week extension.

Let me know what you would prefer 😊

Ngā mihi,

Nick

[redacted]
Kaitohu Tōmua | Senior Policy Advisor
Criminal Law | Policy Group
DDI +64 4 494 9810 | Ext 50810
www.justice.govt.nz

Mon Tues Wed Thur Fri

From: [redacted]@nikkoam.com>
Sent: Wednesday, 1 December 2021 9:40 am
To: aml <aml@justice.govt.nz>
Subject: aml/cft Act review consultation - Request for extension on behalf of BIG group

Good morning I am the chair of the Boutique Investment Group (B.I.G.), which represents between 20-30 non-bank fund managers.

We have drafted a submission but with so many members and many people working inefficiently from home, we would like to request an extension. We also understand that the banks have been granted an extension until 17 December?

Kind regards

[redacted]

[redacted]
General Counsel & Company Secretary

[redacted] | E: [redacted]@nikkoam.com
Nikko Asset Management New Zealand Limited | www.nikkoam.co.nz
PO Box 3892, Shortland Street, Auckland, 1140
Level 17, 48 Shortland Street, Vero Centre, 1010

Confidentiality notice:
This email may contain information that is confidential or legally privileged. If you have received it by mistake, please:
(1) reply promptly to that effect, and remove this email and the reply from your system;
(2) do not act on this email in any other way.
Thank you.

Review of the AML/CFT Act

Submission by BIG on the Ministry of Justice's Consultation Document

16 December 2021

This is submission is by the Boutique Investment Group (**BIG**) on behalf of the Managed Investment Scheme (MIS) Managers listed in Appendix 1. No part of this submission is confidential. Please contact [redacted]@amp.co.nz for any queries.

This submission has three parts:

1. Wider Contexts (New Zealand and MIS Managers) we believe are critical to formulating an optimally designed AML/CFT regime for New Zealand and, in particular, MIS Managers,

2. A thematic response, outlining things we consider are essential to achieve or avoid, and

3. Our detailed responses to many of the questions raised in the Consultation Document.

Wider Contexts

The New Zealand Context

When thinking about what an optimal AML/CFT regime looks like, we need to be aware that what makes sense for one jurisdiction, may not make sense for another. For example, risks and differences between markets justify fundamentally different approaches. Therefore, while it is always right to have regard to "international best practice", we ultimately need to be guided by the question of what approach will work best for New Zealand.

Considering unique New Zealand characteristics is critical when designing our regime. This is because there are striking differences between our New Zealand market and those of the jurisdictions that drive FATF's thinking. In particular, the total population of New Zealand is around 5 million, as opposed to 750-800 million in the EU, over 300 million in the United States of America, and billions in Asia. As such:

- With so much more scale, businesses in other jurisdictions will often be able to sustain a greater level of regulation and mandated process than is the case in New Zealand.
    - Connected with this, the "size of the prize" in larger markets means that businesses will tolerate more oppressive regulation before they exit, whereas New Zealand's markedly smaller market means businesses will question their investments when regulatory requirements outweigh the smaller "prize" on offer in a subscale jurisdiction; and
    - New Zealand is particularly dependent on foreign investment. Therefore, we always need to be conscious of ensuring that New Zealand remains an easy place to do business.
- The markets in larger jurisdictions have more complex products and anonymity and, therefore, are inherently of higher risk.
- Because we lack scale to support the same degree of specialised industry that arises in larger jurisdictions, New Zealand businesses will occasionally do tasks on the side of their normal business as a necessary part of life. Therefore, we do not want to make it impracticable for New Zealand businesses to engage in activities outside the "ordinary course of business".
- We are a nation of subsidiaries, whereas the largest jurisdictions, like the United Kingdom and the United States of America, are nations of head offices. As such,

concepts like conducting Customer Due Diligence on the ultimate owners becomes a more arduous task in New Zealand than it does in larger overseas jurisdictions.
- We perceive our social and international obligations differently to other countries. For example, 'best practice' countries would not have an equivalent to our sense of obligation to help small pacific nations.

Our overall point is that just because a measure makes sense, and doesn't deter business in Europe, America, or Asia, does not mean that the same holds true in New Zealand. The approach that we take to AML/CFT regulations needs to test whether this is the case, both holistically, and in terms of the scores of discrete requirements. Our approach needs to be optimal for a low budget, while also promoting agility and ease of doing business, and we need to be mindful of our social responsibilities that other jurisdictions may not see as being a priority.

The Managed Investment Scheme (MIS) Managers Context

While the goal of law enforcement agencies is to deter and catch money laundering, our goal is to verify/gain comfort that the people we are dealing with are legitimate in a practicable and efficient way.

With that in mind, a large part of MIS Managers' frustration arises where we are obligated to undertake specific, perfunctory, tasks, which impede business. Moreover, often we know that the person we are dealing with is either legitimate or there are better ways of demonstrating that compared to the rigid requirements under current regulation. In particular, our sector spends a great deal of time, effort, and money undertaking ongoing compliance activities on high trust/low risk entities. Some examples to illustrate the point:

- Māori Trusts may have hundreds of trustees, all of whom must be verified. This can be a near impossible task. However, it is often immediately obvious that the source of funds is a Crown Treaty settlement, so there is realistically negligible ML or FT risk.
- Many community trusts with quasi-public sector origins, raise similar issues to those of Māori Trusts.
- We are obliged to carry out checks on high trust entities that are not providing us with any money. Examples are the Public Trust, MMC and BNP Paribas. Similarly, in reverse, such entities are obliged to carry out checks on us, MIS Managers, even though we are licensed under the Financial Markets Conduct Act and any money they receive comes from the client, not us, so it is nonsensical to consider there is ML or FT risk involved.
- Organisations like the AA, Starship, and the Cancer Society require full AML scrutiny.
- Family trusts, which are innocuous, and fairly standard business vehicles in New Zealand, are required to always be treated as high risk.

The regime also does not make it easy for us to contribute to working with agencies to combat AML/CFT. In particular:

- The reporting that we undertake is time consuming and ineffective, due to the difficult interface with FIU and the irrelevant content of templates. It would be much easier, for example, to send a simple message describing the transaction we saw with an explanation of why we thought it was unusual.
- We do not receive any feedback on any reports that we submit, so we do not know what is useful, what is working, what is not, what to look out for, etc.
- There is no coordinated collaboration within like industries.

When considering what the purposes of the AML/CFT Act should be, it would be preferable to add further limbs:

- To enable legitimate business activity in the most efficient way.

- To facilitate collaboration between the public and private sector to combat money laundering and financing of terrorism.

Adding these limbs would provide overarching balance to the framework. Today's regime is essentially non-risk based, excessively prescriptive, and unfit for purpose.

Thematic response

Must Achieve

BIG considers it is essential that the new Act delivers on the following principles:

1. A more risk-based regime

A key deficiency of the current regime is it is not sufficiently risk based. Many requirements are universal, despite some entities such as casinos, money remitters, and banks being rated as high risk by the AML/CFT Supervisors, whereas others are low or medium-to-low risk, such as debt collectors, life insurers, financial advisers and manged investment scheme managers (refer Appendix 2, which identifies these from Sector Risk Assessments). Many of our specific recommendations recurringly point to making requirements risk based and "right-sized", especially where the inherent risk of money laundering (ML) and financing terrorism (FT) is relatively low.

We discuss in "The Managed Investment Scheme (MIS) Managers Context", above, examples of where we are spending large amounts of time and money blindly following processes for high trust entities where this should not be required (e.g., The New Zealand AA), or alternatively we are required to follow a particular approach to gaining comfort that is problematic, where there is an obvious alternate answer to the question (e.g. where we are dealing with Māori Trusts and where identification of trustees is difficult but where source of funds is obvious … a Treaty settlement).

The regime has also made it much harder for some people and businesses to get access to financial services and participate in the economy. Low risk natural person New Zealand customers accessing/using lower risk products need relief. Similarly, the compliance cost and energy by relatively lower risk entities must be stressed because, if costs incurred by those entities are not improving detection, deterrence or prevention of ML or FT, it is wasted time and needless cost to those entities in addition to being a financial services impediment to New Zealanders — in other words a "lose-lose" situation.

2. Sector independence and industry input

Instead of each MIS manager operating in its own silo and replicating the same compliance task in respect of customer, we advocate an outcome whereby a small well-regulated sector with a similar risk profile can collaborate on systems repositories and processes. This would reduce compliance costs, improve the customer experience, and improve the AML/CFT capability of our industry.

As part and parcel of the ecosystem concept, we favour retaining the FMA as our members' supervisor because of its specific knowledge of how our sector's businesses operate and its understanding of risk.

We also want to work in equal *partnership* with our supervisor (e.g., through a joint committee of industry and regulator representatives), in the promulgation of rules, exemptions, practices and guidance for our sector because in future many of the risks and solutions will relate to the implementation of systems. The current model, whereby consensus of supervisors appears the prime measure of success (but regretfully leads to universal expectations that necessarily lead to over-conservative outcomes which are inappropriate for low and low-to-medium risk entities), should be superseded by consensus among the sector-specific supervisor and the supervisor's cohort / sector's participants.

3. A regime that is responsive and agile to changing risks and opportunities

The risks, opportunities, technologies, social needs and business practices that are relevant to the AML/CFT Act regime are in a continual state of change. The law, therefore, needs to be particularly agile to consider new risks, take advantage of new opportunities, or respond to emerging social needs. In our view, the best way that this can occur is if rule-making powers are shared with those at the "coal face", because only they have sufficient interest and knowledge of specific activities to be able to assess risks meaningfully and make decisions quickly and efficiently. An empowered joint sector regulator/Supervisor and committee of industry representatives is how we envisage this operating.

We note under the current model, in which all exemptions have to be signed off by the Minister of Justice, issues that could be dealt with efficiently by a committee (such as the one just described), literally have taken *years* to decide. There are a few reasons for this:

- Through no fault of their own, there are few staff at the Ministry of Justice with knowledge of how financial markets or financial systems work because that is not the sector they work in normally. Putting a Ministry of Justice staff member, with no knowledge of issues relating to a complex/alien financial ecosystem full of jargon, in charge of advising a Minister in respect of an application made by a complex applicant leads to neither good communication nor process; and
- The level of priority that an issue relating to the financial markets would receive by a Ministry of Justice, which has a huge remit, needing to consider such a broad range of social issues affecting life and liberty, has understandably been very low. A devolution of decision-making powers is, therefore, prudent insofar as we consider such decisions are best made when the decision-makers are more focused (i.e., they can better "see the wood for the trees").

Must Avoid

BIG considers it is essential that the new Act avoids these outcomes:

1. Over-regulation and/or confusing regulation

Bad legislation/regulation often has unintended, yet incredibly costly, consequences. As noted in several places in the Ministry's Consultation Document, the New Zealand regime has exceeded FATF baselines. We are encouraged by the Consultation Document's stated aim, i.e., "We want to ensure that any unintended consequences are reduced, if not entirely avoided." (page vi) Prime examples of where over-regulation has added untold inconvenience to New Zealanders, and huge cost to reporting entities, is address verification, which goes beyond the FATF standards. A guiding principle should be to not exceed FATF standards.

Another example/symptom of complexity is rules scattered across lots of different places. Today we have the Act, its regulations, including several exemptions, Codes of Practice, Guidelines, etc. There are several places in the Ministry's Consultation Document suggesting more rules, prescription, Codes, etc. We are concerned that this makes for a much more complex regime. If the primary and secondary legislation are optimally drafted and, especially if risk-based rightsizing is incorporated, there should be little need for exemptions and tertiary rules. It also makes it much easier to formulate guidance if the primary and secondary legislation are "tighter", less complex, and underpin right-sized compliance requirements.

Another aspect of this confusion is there are multiple registers that have some relevance to AML/CFT issues, but none of them work as they should. The prime example of a register that doesn't work in this context is the Financial Service Providers Register (FSPR), which is supposed to:

- Serve as a proxy for identifying businesses that are AML/CFT Act reporting entities (Financial Service Providers (Registration and Dispute Resolution) Act 2008, section 7A(e)), yet it ends up as a *partial* list of AML/CFT Act entities; and
- "[P]romote the confident and informed participation of businesses, investors, and consumers in the financial markets" (section 2A(a)), yet it *undermines* confidence because no one can place any reliance on the bona fides of any of the businesses on the register (because almost any entity can register themselves as almost anything and there appears to be little checking).

Overall, the FSPR appears to serve little purpose other than to aid in levying financial services providers.

One of the keys to making the AML/CFT regime work effectively would be the creation of agreed sources of truth for verifying customers and identifying high trust entities. The revised AML/CFT regime must avoid disaggregation in that regard. We note in several places the inefficiencies and poor customer outcomes delivered by current requirements, which, by design, foster fragmented, inefficient, and inequitable outcomes for all.

2. Perverse constructs

There are aspects of the current regime that simply make no sense. Two illustrative examples are:

- ***Mandatory completion of CDD on statutory court-appointed entities***
  This example shows how poor construction of rules delivers irrational compliance outcomes. In what possible ML or FT scenario should a reporting entity be required to conduct CDD on a judicially endorsed entity? Plainly, the ML/FT risk is effectively zero, so why do the current regime's rules demand that CDD nonetheless be executed?
- ***Completion of politically exposed persons (PEP) screening on natural persons where there is no ability to compulsorily terminate the business relationship***
  To explain this aspect, consider KiwiSaver Schemes. The main requirement/treatment, following identification of a PEP, is for the reporting entity to consider whether to cease the business relationship. This is a reasonable expectation *per se* but only where the product involved is one where the reporting entity has the discretion to make such a determination. Even if, in the case of KiwiSaver (and other superannuation schemes), the reporting entity did want to cease the relationship:
  - It can't because there is no ability to unilaterally cease a KiwiSaver's membership, and
  - Even if there was an ability to cease the relationship, the outcome could be even more perverse because the member could subsequently be reallocated to another unsuspecting KiwiSaver provider.

There are more examples of such constructs in the current regime, which we highlight throughout our detailed response to the Consultation Document's questions, which now follows.

Specific responses

PART 1: Institutional arrangements and stewardship

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?

BIG's Response

For the reasons provided under the heading, The Managed Investment Scheme (MIS) Managers Context, above, consider adding:

> "To enable legitimate business activity in the most efficient way", and
>
> "To facilitate collaboration between the public and private sector to combat anti money laundering and financing of terrorism".

Actively preventing money laundering and terrorism financing

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?

BIG's Response

It depends on what is meant by this, though in principle, the ultimate success of an AML/CFT regime should be measured by its prevention of laundering. If all it achieves is deterrence, but in practice allows most ML/FT to continue, it has not achieved much.

We would support moves to a smarter and more collaborative regime, which would result in us: *(a)* reducing the compliance burdens where there is low risk (e.g., where we are dealing with high trust entities), *(b)* providing better information, more easily, to FIU, and *(c)* thinking about ML/FT risk *intelligently and with common sense*, including prevention, which necessarily would mean less focus on perfunctory compliance.

One example, which illustrates how a tilt to prevention, versus rigid deterrence, could play out is allowing accounts of low or medium-low risk entities to operate without any mandatory CDD until the customer requests a withdrawal. There is no ML/FT to *prevent* until money has been released, and changes such as this would make a big difference to many entities' time and effort and, laudably, such an approach would improve financial inclusion. Indeed, FATF has specifically called this out:

> The AML/CFT regulatory framework in many countries still does not recognize the risk-based approach and offer the possibility of simplified CDD. In such cases, although the country has certain low risk financial inclusion products which would normally qualify for simplified CDD, financial institutions are still obliged to conduct full CDD.
>
> Stringencies in CDD requirements are still among the most important impediments to financial inclusion in some countries.… Sometimes these stringencies arise directly from the AML/CFT law of the country, which is too prescriptive and does not leave any flexibility to bylaws to adopt a risk based approach.[1]

In general, we believe our sector is onboard with the purposes of the Act as they stand. A pivot to a prevention focus would necessarily require investment in technology and resources, which if requirements were poorly designed, could potentially cripple some

[1] *FATF GUIDANCE: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, p. 28.

entities. Many of our members' interactions with their customers are electronic, with no human-to-human contact. These are designed to be fast, reliable, and accurate. They create a better experience for customers (the clear majority of whom are lower risk). Our concern is a blunt requirement for prevention generally would not be commensurate with the risks of ML/FT for lower risk entities/sectors and would inadequately factor the implementation and ongoing costs involved. If it does proceed, requirements should only apply to those sectors considered higher risk of ML/FT.

In conclusion, we are concerned that a focus on prevention, rather than improving the current regime, could manifest as just another layer of compliance-heavy requirements, which achieve little other than to simply slow down legitimate transactions more and exclude more people. This would be clearly an undesirable result. Providing the overall regime design avoids the negative outcomes we outline above, in principle, a tilt in focus to the ultimate measure of success being prevention we would support.

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?

BIG's Response

There is no practical need to make changes to the Act to reflect either of these concepts.

Currently, few, if any, reporting entities would accept money sourced from places like Iran and North Korea, whether or not there is a weapon of mass destruction involved.

If we identified a customer's money as being related to weapons of mass destruction, irrespective of jurisdiction it would be raised immediately with FIU and there would be tools within the existing law to deal with it.

If the AML/CFT Act does attempt to take a position on this issue, it would need to navigate the fact that our four Five Eyes (FVEY) allies all have weapons of mass destruction.

Supporting the implementation of targeted financial sanctions

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

BIG's Response

No, there is no reason to build a confusing industry of compliance in relation to an issue where it is not clear that the people on those sanction lists would ever be likely to touch our country. From a cost-benefit perspective, this cannot be justified for a small jurisdiction. We note that Victoria University of Wellington law professor, Geoff McLay, has referred to related legislation as being "the least successful piece of legislation in New Zealand history."[2]

[2] "The death of NZ's autonomous sanctions regime".

Risk-based approach to regulation

Understanding our risks

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

BIG's Response

Four areas where sharing information should be improved are:

1. Typologies generally.
2. Learnings from successful prosecutions by NZ Police stemming from reporting entities' filing of SARs to the FIU.
3. Joint industry and agency discussions of technologies and systems at a supervisor and relevant industry committee level.
4. Sources of truth and verification information.

There is little of any of these at present, which has negative consequences, including:

- Many reporting entities are not aware of things they should keep an eye out for, and
- Reporting to FIU is, effectively, discouraged when there is no feedback provided.

1.8 Are the requirements in section 58 still appropriate? How could the government provide risk information to businesses so that it is more relevant and easily understood?

BIG's Response

A good Risk Assessment, when it is actively used by a reporting entity, is a very valuable base document. Regretfully, some entities, based on our members' observations from sector meetings, conferences, etc., treat their Risk Assessments as an inconvenience and "compliance" tick-box document.

More could be done to provide exemplar Risk Assessments / anonymised "best in breed" Risk Assessment from reporting entities in sectors. Most feedback in the AML/CFT area tends to be negative, e.g., warnings, fines, dissatisfaction, etc. This should be more balanced. We advocate more active education, calling out good practices, and highlighting the stronger AML/CFT programmes by Supervisors.

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?

BIG's Response

The Act is unbalanced today. Many requirements are universal, focused only on one risk factor rather than the blend of factors, which perhaps ironically, reporting entities must consider in their Risk Assessments.

Throughout this submission we call out many areas where lower prescription for low or medium-low risk entities would produce better outcomes. In principle, we consider that greater focus and prescription on high-risk customers/products/methods/jurisdiction (or, in other words, higher risk entities in the Sector Risk Assessments), and less on the low or medium-low risk entities, is necessary.

Capacity of smaller and larger reporting entities

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

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

BIG's Response

It is not currently right-sized. Especially in regard to transaction monitoring, entities such as smaller Financial Advice Providers, for example, sometimes have little visibility of transactions of their clients because the client may transact directly with a product provider.

As noted above, a more stratified regime would help. In principle, higher risk entities/sectors should have more prescriptive and ML/FT-preventing obligations applied whereas lower risk entities/sectors should be given more discretion as to timing and other aspects of reducing/deterring ML/FT. As noted above, such a regime would be congruent with FATF's view, i.e., optimising AML/CFT regimes to being risk based.

Applying for exemptions from the Act

1.14 Are exemptions still required for the regime to operate effectively? If not, how can we ensure AML/CFT obligations are appropriate for low risk businesses or activities?

BIG's Response

Yes, they are still relevant, see below.

1.15 Is the Minister of Justice the appropriate decision maker for exemptions under section 157, or should it be an operational decision maker such as the Secretary of Justice? Why or why not?

BIG's Response

No, the power should be delegated down to the supervisor level (a committee of supervisor and industry representatives, we maintain), where there is a strong understanding of the activities to which the application relates (see below).

1.16 Are the factors set out in section 157(3) appropriate?

BIG's Response

Largely, yes, though it would be worth adding "practical necessity" and "broader social imperatives" as things to consider.

1.17 Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?

BIG's Response

No. This legislation does not exist in a vacuum. There will be instances where accepting higher risk activities could become a necessity to give effect to a more compelling social need. For example, enabling un/de-banked people to continue to transact, or enabling Pacifica to send money home may not be low risk, but broader social imperatives justify a degree of exemption, nonetheless.

Maybe where an exemption would stand on an assessment of broader social issues, that would be one case where the exemption would be better decided by a Minister.

1.18 Should the Act specify what applicants for exemptions under section 157 should provide? Should there be a simplified process when applying to renew an existing exemption?

BIG's Response

No, individual Supervisors could deal with this through guidance. The case and/or evidence for an exemption should not be highly prescriptive.

1.19 Should there be other avenues beyond judicial review for applicants if the Minister decides not to grant an exemption? If so, what could these avenues look like?

BIG's Response

No. You *could* conceptually have a framework where an exemption may be referred to the Minister if the expert body/supervisor declines the application. However, a such a review is not normally considered helpful and, moreover, would consume a lot of valuable time in preparing even more submissions, plus the time required to consider the "appeal".

Generally there will be better results if you can engender constructive engagement between the applicant and decision maker. This is less likely to occur if the decision maker is thinking about an appeal body potentially overruling them.

1.20 Are there any other improvements that we could make to the exemptions function? For example, should the process be more formalised with a linear documentary application process?

BIG's Response

The FATF examples provided in the Consultation Document are clearly missteps, rightly called out. However, on the flip side, as an example, there are instances where low risk person/product/method/jurisdiction exemptions do not proceed due to being too onerous. (We have an example, should the Ministry wish for an illustration of this in practice, where a leading law firm recommended against seeking an exemption because it would be too much time/cost and effort, despite the merits of the proposed request being very compelling).

Somehow the settings need to be better framed for exemptions so that it is clearer to applicants, and to the MoJ, what should be straightforward exemptions.

However, if the most burdensome parts of the regime (which are also ones that do little to prevent ML or FT) are relaxed, the need for exemptions should reduce markedly, noting we should aim for a low number because they are, by their nature, time-consuming and inefficient insofar as any request to Government agencies is inevitably, albeit necessarily, a bureaucratic one.

Simply put, the need for, and the sheer number of exemptions, is a symptom of the overly complex and not-fit-for-purpose regime. If the stratified, risk-based, approach advocated by our submission is adopted, the need for exemptions would reduce substantially, in addition to the benefits of: *(a)* increased prevention and deterrence of actual ML/FT, and *(b)* reduced annoyance, inconvenience, and cost to the clear majority of law-abiding New Zealanders.

Also, we observe that questions 1.14-1.20 do not consider a key measurement: success should be having an exemptions process, but one that entities seldom feel the need to invoke (because the default settings of the regime *work well*).

That said, there will always be a need for exemptions because markets and business practices evolve. So, there will always be new risks and opportunities to address.

As we note at the start of this submission, dealing with change in the most efficient way is strongly recommended. This means rule making powers, including exemption powers (where practicable), should be delegated to bodies closer to the "coal face", who have sufficient interest and knowledge of specific activities to be able to assess the risks and

make decisions quickly and efficiently. The joint sector regulator/Supervisor and industry committee, which we advocate, would be best placed to consider at least some exemptions.

We note under the current model in which all exemptions have to be signed off by the Minister of Justice, issues that could be dealt with by a committee comprising of a sector regulator/Supervisor and industry representatives within a month, have literally taken several years to decide. There are a few reasons for this, which are detailed, above, under the heading "3. A regime that is responsive and agile to changing risks and opportunities"

We are opposed to the process becoming "more formalised with a linear documentary application process". In our experience, the key to a good regulatory process is where both sides can engage and share information in a constructive and informal way. This is especially relevant where there may be a solution that satisfies the needs of both sides, which looks different to the original request for an exemption.

Part of the problem with the current process is that Ministry of Justice staff have not had the skill and confidence to engage with participants in our sector and have defaulted to defending matters, citing "process". In contrast, a more successful exemption process, such as that operated by Financial Markets Authority under in its Financial Markets Conduct Act remit, exhibits a significant amount of ongoing constructive discussion between the parties and, more often, better outcomes.

Mitigating unintended consequences

Financial inclusion or exclusion

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?

BIG's Response

It is incongruent that a personal account with a $1,000,000 opening or ongoing balance requires CDD to the same degree as one of $1,000. To reduce the impact on those impacted (i.e., financial inclusion-wise), consideration should be given to a *de minimis* level whereby CDD is not mandatory. There is next to no risk from an AML/CFT perspective from low value accounts. Applying a risk-based approach, demanding CDD for low balances should be seriously looked at. This would also aid financial inclusion because for many people with low new wealth and low balance accounts the impediments of CDD drive exclusion more that they reduce ML / FT.[3]

Another unintended consequence is duplication of efforts in respect of the same customers, in respect of the same transaction. For example, if you purchase a house, you will typically be required to undergo the same AML checks by both the real estate agent and the lawyer. Enabling sector regulators, with industry representatives, opportunities to remove such duplication from their practices where relevant, we advocate strongly.

[3] Indeed, we recommend detailed consideration of the examples provided by FATF of other jurisdictions' common-sense approaches to account opening and operation of low value accounts. From an incumbent New Zealand AML/CFT regime perspective, such approaches may be considered radical, yet they clearly illustrate that an AML/CFT regime can operate with "ands", i.e., achieve solid ML/FT outcomes as well as inclusion for the people for whom the current regime in New Zealand is frustrating at best, and exclusionary at worst. Refer: *FATF GUIDANCE: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, pp. 84-92.

The role of the private sector

Partnering in the fight against financial crime

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?

BIG's Response

BIG considers there are many opportunities to "partner" with the private sector. We consider these should include:

1. As noted above, a supervisor and relevant industry representatives could form a committee to exchange information and experience between public and private sector, promote best practice, co-author guidance, and decide some exemptions.
2. Sector-specific and rightsized guidance and requirements built by the Supervisor in partnership with each sector's entities. There is too much isolated Supervisor decision-making today, an example being the change to expired passports, which was not given sufficient consideration as to the risk versus cost of compliance that resulted.
3. Allowing blanket sharing of CDD or PEP screening information and sharing/relying on others reporting entities' CDD/PEP completion results (without any "intermediaries" exemptions). If that required a Privacy Act carve out, so be it.
4. Developing a Pharmac-style model for CDD and PEP, either overall or for each Supervisor's sectors. The amount of money wasted by New Zealand entities on CDD and PEP screening, the latter mostly with foreign corporate services providers, is remarkable. There is a huge opportunity to (semi-)centralise these services to reduce direct and indirect costs and standardise on appropriate tools. To illustrate, a contract for *all* PEP screening for *all* of New Zealand would deliver: *(a)* consistency, *(b)* be a small fraction of the cost incurred by reporting entities today, and *(c)* would remove the need for every entity to evaluate the quality for the screening providers (demanded by Supervisors). Government needs to remember that AML/CFT compliance is not something entities are doing for their own benefit, so initiatives that reduce compliance cost, standardise on solutions, etc., should be considered.

If the suggestions above do not get taken up, a further idea (though not a "partnership" one) is to enable validation of customers' data against the Government's data sources directly. Why should reporting entities, *doing the Government's work* (in checking whether someone is bona fide for AML/CFT purposes) not be able to send name and date of birth directly and have confirmation returned that either the information has a match or does not? There should be few privacy concerns in this because, if the person has provided their information to the reporting entity, there is nothing being disclosed in simply verifying that the customer's data (name and date of birth) is actually valid.

Helping to ensure the system works effectively

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

BIG's Response

Perhaps, though only if it would lead to actual changes should this be considered. If it is just feedback that will go nowhere or not lead to any changes, such a mechanism would only waste submitters' time.

This would more likely be effective if some rule-making powers were delegated to a lower level, so that a lot of the detail could be tweaked by a supervisor. Part of the problem with achieving regulatory change is if it needs to go all the way to the top and occupy Ministerial time.

Powers and functions of AML/CFT agencies

Powers of the Financial Intelligence Unit

Allowing information to be requested from other businesses

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

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

Providing for ongoing monitoring of transactions and accounts

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?

BIG's Response

Provided it was rarely exercised, this power if it *prevented* laundering or terrorism, could be justified. However, we consider that the bar would need to be very high, perhaps requiring judicial authorisation to demand such a treatment of the subject of the request and the burden on reporting entities. There is an analogy for such an approach in lawful interception legislation in relation to telephone records, etc.

What we would not support is an unfettered right for FIU to request information from businesses at a whim, regularly, or on an ongoing basis, without any clear justification that actual prevention of ML or FT is necessary. One possible way of ensuring that the exercise of power was not being undertaken lightly would be if the FIU was required to fund the cost of such provision of information.

At a practical level, part of the current problem is that FIU does not make it easy for participants to provide it with information because of its problematic and one-size-fits-all systems as well as almost no meaningful feedback on our suspicious activity reporting.

If we could foster/enable better free and frank ongoing general dialogue about what each side was seeing, then that may achieve a better outcome

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?

BIG's Response

If this power was provided to the FIU, or the Police specifically, it would put reporting entities in an impossible situation vis-à-vis tipping off. What could a reporting entity possibly say to the client whose account was locked? Would it be, "*Sorry, we're having trouble making a withdrawal for you today?*"

Someone needs to think carefully about this because it seems very much like wanting your cake and eating it too. Further, it would put more burden and stress on reporting entities' staff, which should not be downplayed nor ignored.

The only way this power should be allowed is if the treatment is overt: i.e., the customer, if they enquire, is told *explicitly that the FIU has frozen their account* and that the provider has no option but to enforce the direction of law enforcement.

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?

BIG's Response

Targeted financial sanctions should be carefully considered as there is a real likelihood of creating undue compliance cost in any monitoring regime. Some entities have almost no probability of having any transactions subject to it. Specific carve outs for some industries should be considered, e.g., those who only transact via NZ banks, because the banks themselves should sufficiently identify any TFS issues. (NB: That would make the regime much like that for PTRs.)

A centralised agency for this limited area should be tasked with managing it; that is, it should not be added to the three supervisors' remits. That is because they already struggle with the peripheral things like PTRs (in terms of understanding and guiding their reporting entities).

Secondary legislation making powers

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

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

Codes of Practice

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?

BIG's Response

Widely distributed law is difficult to get fully across. The experience to date, if the Amended Verification of Identity Code of Practice (IVCOP) is used as an exemplar, is that Codes of Practice via Supervisors should be eliminated. Their development (in requiring consensus of the Supervisors) is glacial, and their value is limited. In fact, the IVCOP was worse than having no guidance/a Code at all.

Unless Codes are simple, clear, and flexible (i.e., truly risk-based), and built-in consultation with sectors/reporting entities (who should have some form of veto right if a proposed Code is manifestly unhelpful or more than the law demands), they do not add value.

Forms and annual report making powers

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

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

BIG's Response

In theory, devolving the form-making and reporting to a clearer, more flexible (risk-based), and collaborative (with reporting entities) process is good. The main challenge with such devolution is that these reports balloon in scale/extent and more compliance burden is the result rather than less. If the requirement is only for *demonstrably necessary* information to be able to be requested (with some form of challenge available), this could work.

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?

BIG's Response

Proliferation/fragmenting of the law/rules for AML/CFT would be a backward step. The regime needs better risk-based principles-based requirements, not increase prescription. This proposal should not be progressed.

Information sharing

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?

BIG's Response

1) Provision of information to other organisations for AML/CFT Act purposes

The isolated nature of SARs is a frustration to diligent reporting entities. There is never any feedback on our SARs meaning we have little idea whether we are wasting time reporting things or not.

Privacy issues should not trump the aim of preventing laundering (because, by its nature, criminals want to be private!). This should extend further into annual feedback to entities on their reports, including a summary of the number/percentage that resulted in a prosecution / investigation / or were just "filed" with no action. That would provide each reporting entity that filed SAR(s) with insight as to whether they are reporting too much or too little. For example, if a reporting entity reported 12 SARs in a year and all were "filed", the reporting entity could rightly conclude that it has probably been wasting their, and FIU's, time. Such a

change would ultimately reduce compliance burden by helping entities appreciate what SARs are likely to be of interest to the FIU.

2. Provision of information to other organisations for non-AML/CFT Act purposes

If the intent is to create an environment of collaboration between industry and FIU (ultimately) to combat ML/FT, the free and frank flow of information could be compromised if there was no clarity as to which other entities' information disclosed to FIU could be passed on to and for what purpose.

In addition, the proposal that information collected seemingly for one purpose (but used for another) brushes up uncomfortably against principles of privacy.

If the FIU were to become a "backdoor" way of other agencies harvesting information, then, at a practical level, that would likely result in more "fishing expeditions" and more unjustifiable requests for information coming from FIU.

In conclusion, we would want to know a lot more before we could consider supporting this.

Data matching to combat other offending

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?

BIG's Response

If the aim of the regime is to *prevent* laundering, not just deter or detect it, open sharing of PTRs and SARs should be implemented without pause. Businesses are unlikely to reduce SAR reporting because of concerns of inappropriate sharing and, in fact, the fear that this *could* occur may be sufficient deterrent for any misuse of SAR data by agencies.

Licensing and registration

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?

BIG's Response

Provided existing licensed entities (e.g., FAPs, MISs, DIMS, Banks, Licensed Insurers, and so forth are *de facto* registered, this would be fine. Under no circumstances should an additional licence be required of financial services licensees who already have licences — that would serve no purpose and would needlessly add to compliance costs.

An *everyone else* regime, for those who do not already have a financial services, insurance, or banking licence, but have AML/CFT obligations, could be considered if it washes up those remaining entities in a way that makes things more efficient and adds to fitness and propriety, rather than adding burden to today's already over-licensed entities.

However, a practical question is whether anyone is resourced to undertake a meaningful AML licencing process for the vast number of reporting entities that exist outside the prevailing licensing regimes.

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?

BIG's Response

This has already been mostly answered: perhaps, but only *(a)* if it does not add to any existing licensees' burden insofar as requiring yet another licence and *(b)* only if the rewards of implementing such a regime would be value accretive — as there are a *lot* of reporting entities in existence, it is difficult to imagine a public sector entity sufficiently resourced to licence the universe of entities in a way that we expect would deliver any kind of meaningful value. It is far more likely that such a regime would achieve nothing other than a perfunctory levy-enabling register, much like our observations of the deficient FSPR, discussed above.

Registration or licensing fee

1.60 Would you support a levy being introduced for the AML/CFT regime to pay for the operating costs of an AML/CFT registration and/or licensing regime? Why or why not?

1.61 If we developed a levy, who do you think should pay the levy (some or all reporting entities)?

1.62 Should all reporting entities pay the same amount, or should the amount be calculated based on, for example, the size of the business, their risk profile, how many reports they make, or some other factor?

1.63 Should the levy also cover some or all of the operating costs of the AML/CFT regime more broadly, and thereby enable the regime to be more flexible and responsive?

1.64 If the levy paid for some or all of the operating costs, how would you want to see the regime's operation improved?

BIG's Response

No. There are already huge licensing costs today. For example, some of our MIS licensee members pay over $500,000 p.a.

In principle, we also consider that charging for an AML/CFT licence is odd: whereas for licences such as banking, insurance, and manged investment schemes there is a clear benefit to the entity from the activities the licence enables, there is no direct benefit to an entity from fulfilling its AML/CFT obligations. An analogy is driving versus paying tax: expecting an individual to have a licence to drive a motor vehicle (which provides benefit to them) is reasonable, whereas we would not expect that individuals request a licence to pay tax to the Government!

Another, more formal, way of expressing this point is that the normal principled approach to regulatory cost recovery is that the Crown should pay for public good benefits of a regime and the private sector should pay for benefits that flow through to their customers. In this instance, as all the direct benefits flow through to the greater public good, the costs should fall on the Crown.

PART 2: Scope of the AML/CFT Act

Challenges with existing terminology

"In the 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?

BIG's Response

At a practical level, a business doing an extraordinary activity will have neither a risk assessment and compliance programme covering that activity nor necessarily be overseen by the applicable Supervisor. Building such regulatory architecture is not justified for occasional activities. The consequence of extending AML/CFT obligations to non-ordinary course of business activities, therefore, is that you stop businesses from doing everything that is outside their ordinary scope business.

As New Zealand is a small jurisdiction, enabling businesses to step outside of their normal activities infrequently is, in reality, a necessity. This is because there is no established industry performing all activities. The carve out for non-ordinary course of activities is an important feature in this jurisdiction (not relevant to other jurisdictions where they do have a range of businesses performing obscure tasks in their ordinary course of business).

We conclude, "ordinary" *should not* be removed.

Businesses providing multiple types of 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?

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?

Refer comments to 2.1–2.3, above.

"Managing client funds"

Overlap between "managing client funds" and financial institution activities

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?

BIG's Response

It is unclear to us what/whether there is problem at all with this "overlap".

"Sums paid as fees for professional services"

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?

—

"Engaging in or giving instructions"

2.10 Does the current definition appropriately capture those businesses which are involved with a particular activity, including the operation and management of legal persons and arrangements? Why or why not? How could it be improved?

2.11 Have you faced any challenges with interpreting the activity of "engaging in or giving instructions"? What are those challenges and how could we address them?

—

Definition of financial institution activities

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?

BIG's Response

Consideration should be given to the repeal or otherwise significant overhaul of the Financial Service Providers (Registration and Dispute Resolution) Act 2008, which was not amended significantly despite being in scope of the FSLAB/FSLAA review of financial advice licensing.

Today, the FSP operates contrary to New Zealand's interests by providing a false appearance that entities on the register are *regulated*. It also does not adequately cover the scope of entities covered by the AML/CFT Act. Therefore it serves little practical use, especially in the context of coverage of AML/CFT reporting entities.

If retained or otherwise not overhauled, however, aligning terminology between the AML/CFT Act and the FSP(RDR) Act is probably a simple task and would reduce potential confusion.

High Value Dealers

Definition of "high-value dealer"

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

2.15 What do you anticipate would be the compliance impact of this change?

—

Exemption for pawnbrokers

2.16. Should we revoke the exclusion for pawnbrokers to ensure they can manage their money laundering and terrorism financing risks? Why or why not?

2.17. Given there is an existing regime for pawnbrokers, what obligations should we avoid duplicating to avoid unnecessary compliance costs?

—

Appropriate cash transaction threshold

2.18 Should we lower the applicable threshold for high value dealers to enable better intelligence about cash transactions? Why or why not?

2.19 If so, what would be the appropriate threshold? How many additional transactions would be captured? Would you stop using or accepting cash for these transactions to avoid AML/CFT obligations?

—

Stored Value Instruments

2.20 Do you currently engage in any transactions involving stores of value that are not portable devices (e.g. digital stored value instruments)? What is the nature and value of those transactions?

2.21 What risks do you see with stored value instruments that do not use portable devices?

2.22 Should we amend the definition of "stored value instruments" to be neutral as to the technology involved? If so, how should we change the definition?

BIG's Response

Although we do not engage in transactions involving "stored value instruments" it appears that there is a need to expand the definition so that it is relevant to 2022 and beyond. For example, in addition to the example provided ("email vouchers"), in essence all cryptocurrency wallets and/or private keys could fall within the policy intent of the definition. Such digital assets appear to be ignored by this consultation. Despite some being almost impossible to regulate or track (e.g., even if some/all were banned in New Zealand they could easily be used via VPN connections transacting in foreign jurisdictions), it may be optimal to use a term such as "stored value means" to make the definition wide enough to cover essentially anything.

Notwithstanding the technical improvements which could be made to the definition, included "stored value means", or similar, is unlikely to assist in preventing ML/FT given many such "means" cannot be tracked at all. Some cryptocurrencies, unlike Bitcoin (which is a regularly used synonym yet is only one of thousands of such stores of value), are entirely private and untraceable.

Potential new activities

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

2.23 Should acting as a secretary of a company, partner in a partnership, or equivalent position in other legal persons and arrangements attract AML/CFT obligations?

2.24 If you are a business which provides this type of activity, what do you estimate the potential compliance costs would be for your business if it attracted AML/CFT obligations? How many companies or partnerships do you provide these services for?

BIG's Response

As a matter of principle, regulatory regimes should be neutral as to the corporate structure of the reporting entity.

While it may make sense to allow a business to choose its corporate structure to determine what level of exposure it is prepared to take on in its commercial interactions (which contracting parties can either choose to accept or reject), it doesn't make sense to allow some types of business to opt out of the same level of regulatory duties as other businesses. Therefore, either directors of companies and all their equivalents in other types of entity should be exposed to liability, or none of them should be exposed to liability.

A broader concern in the corporate world is that directors are facing unprecedented increases in personal accountability for so many regulatory issues that it is having a chilling

effect on many companies being able to get directors with the right skill sets that they need to succeed as a business. Further, in their roles, directors are becoming distracted from the core business of the companies that they provide governance for, due to all the regulatory issues that they must factor. This is potentially contributing factor to New Zealand having low levels of productivity relative to other countries, despite its staff working relatively hard. Therefore, the policy question should be to think about how important AML/CFT compliance is, including against *other* forms of compliance that directors should be focusing on (e.g., health and safety, privacy, cyber security, etc.), versus the core regulatory obligations relating to their business, which for MIS Managers is Financial Markets Conduct Act compliance.

The secretary of a company, especially, should not be liable because: *(a)* the company secretary is commonly just someone who helps a board with its administrative tasks such as, keeping minutes of board meetings, setting agendas and filings etc. They have no special status in law, and there is no obligation for a company to have a company secretary, and perhaps more importantly, *(b)* Company secretaries usually have no oversight of AML/CFT functions within a business, nor any day-to-day visibility of a company's finances. This proposal possibly misunderstands what a company secretary's role is in the New Zealand context.

Criminal defence lawyers

2.25. Should criminal defence lawyers have AML/CFT obligations? If so, what should those obligations be and why?

2.26. If you are a criminal defence lawyer, have you noticed any potentially suspicious activities? Without breaching legal privilege, what were those activities and what did you do about them?

2.27. Are there any unintended consequences that may arise from requiring criminal defence lawyers to have limited AML/CFT obligations, that we need to be aware of?

BIG's Response

The overarching duty of any lawyer is to act as a trusted advisor to the client. It is important that the AML/CFT Act does not cut across this function.

While lawyers' obligations are primarily a matter for the New Zealand Law Society to comment on, our preference would be to know that our lawyers are there to act for us and that they are not there to act for the law enforcement agencies in the event that we ever need to rely on them to defend us for any reason.

Non-life insurance businesses

2.28 Should non-life insurance companies become reporting entities under the Act?

2.29 If so, should non-life insurance companies have full obligations, or should they be tailored to the specific risks we have identified?

2.30 If you are a non-life insurance business, what do you estimate would be the costs of having AML/CFT obligations (including limited obligations)?

BIG's Response

The risk of laundering via general insurance is so remote it is not worth considering extending the regime/burden to those entities. The main risk in insurance is not what is outlined; from past experience (when our DBG had a Life Insurer member) it is loans on policies (regularly repaid and another loan taken) where the most risk lies. Unless it can be demonstrated that insurance really is a risk worth addressing, based on overseas typologies validated as applicable to the NZ context, we consider that there should be no extension of the regime into insurance. This view aligns with FATF's:

> In some cases this concern about the assessors causes the country to be even more onerous than the FATF recommendations. **Examples of such requirements include the coverage of**

> **the general insurance products in AML/CFT regime, requirements to verify the address**, document the purpose, or provide a Tax ID number or secondary ID document regardless of the amount and risk level of the transactions.[4] [*our emphasis*]

Note the reference to "verify the address" too. As MoJ has observed, verification of address is one of the unnecessarily onerous requirements today, which seems almost certain to be unwound with this review. General Insurers should absolutely *not* be similarly unnecessarily swept into the regime.

Including all types of Virtual Asset Service Providers

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?

BIG's Response

Extending to these is fine from a *box-ticking-with-FATF* perspective, however, the true AML/CFT risk is the iceberg beneath the tip being addressed. Virtual asset service providers will not be used by any even slightly savvy launderer. Launderers will almost certainly do direct wallet-wallet (peer to peer) transfers of value, which (in some blockchains, though not Bitcoin) are totally anonymous. This should be kept in mind because if the aim is to prevent or deter laundering, the proposed change is not likely to have much impact.

Combatting trade-based money laundering

Preparing or processing invoices

2.33 Is the Act sufficiently clear that preparing or processing invoices can be captured in certain circumstances?

2.34 If we clarified the activity, should we also clarify what obligations businesses should have? If so, what obligations would be appropriate?

Preparing annual accounts and tax statements

2.35 Should preparing accounts and tax statements attract AML/CFT obligations? Why or why not?

2.36 If so, what would be the appropriate obligations for businesses which provide these services?

BIG's Response

There are over 560,000 companies incorporated in New Zealand, and vast numbers of small accounting businesses helping out equally vast numbers of SMEs across New Zealand.

The logistics of attempting to bring every entity that helps with accounts into the regime, let alone some sort of AML assessment as being incorporated into the preparation of every tax set of tax statements, would be a monumental challenge and unlikely provide any meaningful value.

Non-profit organisations vulnerable to terrorism financing

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?

—

[4] *FATF GUIDANCE: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, p. 28.

Currently exempt sectors or activities

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

—

Internet auctioneers and online marketplaces

2.40. Should the exemption for internet auctions still apply, and are the settings correct in terms of a wholesale exclusion of all activities?

2.41. If it should continue to apply, should online marketplaces be within scope of the exemption?

2.42. What risks do you see involving internet marketplaces or internet auctions?

2.43. If we were to no longer exclude online marketplaces or internet auction providers from the Act, what should the scope of their obligations be? What would be the cost and impact of that change?

—

Special remittance card facilities

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

2.45 Is the exemption workable or are changes needed to improve its operation? What would be the impact on compliance costs from those changes?

2.46 Do you consider the exemption properly mitigates any risks of money laundering or terrorism financing through its conditions?

—

Non-finance businesses which transfer money or value

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

—

Potential new regulatory exemptions

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

BIG's Response

Consider making the managing intermediaries exemption a regulatory exemption so that it lasts indefinitely.

Acting as a trustee or nominee

2.49 Do you currently use a company to provide trustee or nominee services? If so, why do you use them, and how many do you use? What is the ownership and control structure for those companies?

2.50 Should we issue a new regulatory exemption to exempt legal or natural persons that act as trustee, nominee director, or nominee shareholder where there is a parent reporting entity involved that is responsible for discharging their AML/CFT obligations? Why or why not?

2.51 If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?

—

Crown entities, Crown agents etc

2.52 Should we issue a new regulatory exemption to exempt Crown entities, entities acting as agents of the Crown, community trusts, and any other similar entities from AML/CFT obligations?

2.53 If so, what should be the scope of the exemption and possible conditions to ensure it does not raise other money laundering or terrorism financing vulnerabilities?

BIG's Response

Yes, all Crown entities, QANGOs and NZ Court-appointed administrators and, indeed, anyone in an official or delegated governmental or judicially enabled role should be exempt. It is ludicrous that entities waste time conducting CDD on these sorts of entities. If it is really necessary, keep them in scope of SARs by all means, but specifically remove any requirement to prove who they are other than having official letterhead/email addresses/court orders, etc. Validating ID should not be required.

Low value loan providers

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

2.55. If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?

Territorial scope

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?

BIG's Response

Only provided it is clear and does not produce perverse outcomes. For example, the Australian regime technically puts any legal entities in a conglomerate who offers products of the type captured by that regime (despite not being issued under its jurisdiction) as "in". Such perverse outcomes must be avoided as they consume far too much time arguing with lawyers about why the law makes no sense.

At least part of the activity by the entity should occur in New Zealand. At a practical level, the issue is whether the Government can realistically oversee and/or enforce against a person who is not within the jurisdiction.

PART 3: Supervision, regulation and enforcement

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?

BIG's Response

The model has the benefits that you tend to deal with the regulator/supervisor with whom your licensing obligations rest (be it for MIS, so FMA, or insurance, so RBNZ).

Where the current model falls down is in relation to the glacial developments / paralysis that besets the Supervisors when working collectively. The necessary consultation and consensus among them to reach decisions probably explains why things like the IVCOP are so slow, sub-optimal, etc., when they are produced.

For reasons discussed above, we would welcome having a sector-focused regulator/supervisor with decision-making ability in conjunction with its sectors, not with other supervisors. In many instances, the nature of the entities regulated by the DIA are of quite a different nature to those regulated by the FMA and Reserve Bank. Therefore, we are currently spending a significant amount of time attempting to create consistent processes between activities that do not relate to each other in any meaningful way.

The AML risks and policy considerations for a casino, for example, are entirely different to the risks and considerations of regulating a KiwiSaver scheme. The best approach would be to decouple further and generally allow sectoral regulators to regulate their own sectors in their own way, unless there is some kind of particular cross-over for an issue.

Consideration could be given to reduction in the number of Supervisors from three to two because when the current regime initiated, the FMA had comparatively little engagement with entities licenced by the Reserve Bank (banks and insurers). So having the RBNZ supervise those entities for AML/CFT made sense. That has now changed, with FMA engagement with these entities ongoing, significant and growing. A single supervisor for financial institutions and one for non-financial institutions may be a suitable model. This could help achieve efficiencies (e.g., AML monitoring could be included in a wider monitoring engagement).

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?

BIG's Response

As noted above, why does it make sense to attempt to achieve consistency between the way that you regulate a casino and the way that you regulate a KiwiSaver provider? They are not only totally different in terms of their potential for AML/CFT risk, but the social considerations are entirely different. For example, generally speaking Government wants all New Zealanders to have KiwiSaver, whereas there is no similar social imperative to give all New Zealanders access to a casino.

Even within a sector there is room for more nuance in how Supervisors treat their sector/sub-sectors, particularly within the Department of Internal Affairs' wide range of reporting entities. Sector-specific guidance may be the answer? Today's regime does tend to

be one size-fits-all and that inevitably causes overcooked requirements for lower risk entities with lower risk customers.

Powers and functions

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

—

Inspection powers

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?

BIG's Response

The FMA (the Supervisor that we are familiar with) has had a long history of conducting both desk-based reviews and site visits of its participants, as appropriate, with no difficulty.

We believe that, in most instances, this engagement has been carried out largely without the exercise of formal powers. However, in some instances the FMA has supplemented its approach where needed with the powers to: *(a)* requisition any information that it needs (pursuant to section 25 of the Financial Markets Authority Act 2011) and *(b)* enter and search any place, vehicle or thing (pursuant to section 29 of the same Act).

If the FMA were to be dealing with an entity whose office premises also serves as a dwelling, and the circumstances meant that negotiated access was not workable, our expectation would be that it would require production of information in the first instance (section 25), and if that raised concerns it would then seek to invoke section 29, if FMA needed to go onsite, which requires third party endorsement as a check.

Therefore, it is not clear whether there is a gap in formal legal powers that needs to be filled, at least for one supervisor.

Approving the formation of a Designated Business Group

3.9 Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient?

3.10 Should supervisors have an explicit role in approving or rejecting the formation of a DBG? Why or why not?

BIG's Response

The benefits in having a DGB are fairly limited so, unless they were to become significant, there seems little need for a rejection/approval process. Today, key benefits include reducing the annual reporting burden and sharing processes, which should not require any elaborate approval process; that would be administration for administration's sake.

If an entity is willing to take responsibility for the AML compliance of another entity, that should be largely enough. As a comparator, the FAP licensing regime allows for entities to work under the umbrella of a FAP. This could serve as a model for AML compliance too. For many low-risk entities, the costs of compliance are significant – and their compliance maturity can be poor. Relaxing the DBG eligibility criteria may be a route to uplifting the compliance efforts of many reporting entities.

Regulating auditors, consultants, and agents

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?

BIG's Response

If there are specific concerns about the quality of audits those have been identified by the Supervisors. What appears missing is an ability to ban an auditor who is found to be inadequate. That, along with making a requirement to be re-audited if the current auditor is later banned, should be enough incentive for auditors to "up their game".

A practical observation is that there needs to be enough AML/CFT auditors to service the universe of AML/CFT reporting entities.

Following the inclusion of lawyers, real estate agents and some accountants into the regime, it seems as though there is already a shortage of AML/CFT auditors. If mandatory professional standards/licencing was to be introduced and the number of reporting entities was to be expanded, then the market may not be able to cope, notwithstanding the recent reduction in frequency to every three, rather than two, years.

Another thing to factor is who would audit the auditors? There would need to be some form of licencing or approval regime for that to happen, and that would set a high hurdle that would be of limited benefit, with the result that larger consulting firms would reap the benefit of the higher costs of entry.

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?

BIG's Response

Although the concept of applying a penalty where a consultant's advice is illegal or manifestly inadequate seems straightforward, we consider it may not be so in reality and this is an area that does not require more prescription.

The reality is the responsibility for a reporting entity's outputs remains with the reporting entity. An industry is also likely to exchange views as to which consultants are good and which are not. This creates a basis for industry to police itself as far as consultants are concerned.

A framework for consultants would require someone to set and enforce standards. It is not clear that such an activity would be net positive if the outcome is to deny the market access to consultants.

Agents

3.18 Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for?

BIG's Response

Yes, for example, some of our members use agents for gathering CDD from mutual customers.

3.19 Do you currently take any steps to ensure that only appropriate persons are able to act as your agent? What are those steps and why do you take them?

BIG's Response

It is a common situation in the financial sector that a customer will be dealing with more than one reporting entity in respect of the same transaction. For example, in the case of a customer simply choosing a KiwiSaver investment, all the following entities may be involved:

- A financial adviser recommending the product working for a FAP;
- A MIS manager offering the product; and
- A custodian receiving and holding the funds.

It doesn't make sense, from either a customer centric perspective or from a risk perspective, to have three sets of AML checks carried out on the same person at the same time going on in silos. Therefore it is very common to have a customer onboarding process that is in some way shared between the manager and the FAP. Depending on the business model, in some scenarios the FAP appoints the MIS manager as its agent, and in others the MIS manager appoints financial advisers (or their FAP) as its agent.

The control normally used in this situation are that any agents will be reporting entities in their own right and will have a close business relationship (for example many MIS managers will require FAPs to go through some form of training before they are allowed to recommend particular products). Another practice is, in some arrangements, that the results of identify checks, the results of a third party's reports, etc., will be pass along.

It is also common for reliance on the managing intermediaries exemption for underlying customers where an institutional customer invests in funds and has underlying customers.

Our members also use various businesses, e.g., Cloudcheck, to assist with customer verification.

3.20 Should there be any additional measures in place to regulate the use of agents and third parties? For example, should we set out who can be an agent and in what circumstances they can be relied upon?

BIG's Response

Currently the principal remains liable for the conduct of the agent, with the consequence that the use of agency has not necessarily grown as much as it should have done. For example, the concept of a central business doing AML/CFT checks that all our industry uses has often been discussed but it has never been practicable, in part because of the liability clause.

It would be useful if supervisors could work with businesses to facilitate more effective and efficient use of agents in the regime.

Offences and penalties

Comprehensiveness of penalty regime

Allowing for intermediary enforcement options

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 noncompliance 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?

BIG's Response

If an overhaul of potential penalties available to Supervisors is considered necessary, we would want those potential penalties to be proportionate. Supervisors should not be reaching for their enforcement tool kit just because they can. Any changes to the penalty regime must include corresponding changes to checks and balances to ensure that their application is fair in practice.

Allowing for higher penalties at the top end of seriousness

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?

BIG's Response

It is difficult to say that the offences and penalties are insufficient, given that the supervisors have only recently started to use more of their "tool kit".

Early indicators are that larger entities are more vulnerable to any exercise of power because of the potential damage to brand if they are publicly called out. As a case in point, the Australian CEO of recently resigned following the organisation being (rightly) called out.[5] Such an outcome could also occur in New Zealand.

It is important that there is not a proliferation of penalties for trivial or low risk failings, however. In cases such as Westpac, above, where egregious systemic failing to meet AML/CFT obligations occurred it is appropriate. We would not want to see simple, non-systemic, and especially administrative things such as inadequate annual reporting, where actual ML or TF was not likely to have occurred, be penalised.

Sanctions for employees, directors, and senior management

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?

BIG's Response

This needs to be carefully considered as it would add a further burden to directors. Obligations for which directors can be held personally liable for, will inevitably become prioritised over and above other obligations and functions of an organisation (and there are

[5] https://www.theguardian.com/australia-news/2019/nov/26/westpac-chief-executive-brian-hartzer-resigns-over-money-laundering-scandal

only so many issues that can reasonably be afforded priority consideration). Therefore, we need to think about where AML/CFT should sit in the order of priorities that directors have against other matters that are considered so important as to potentially attract director liability including: health and safety, competition law, reckless trading, fraud, cyber security, issuer regulations, licences' obligations, etc.

However, Compliance Officers must be protected where their recommendations, if ignored, would otherwise have prevented a harm that is later identified.

With large companies, the threat of publicly being forced to resign in a career-ending way is in itself quite a powerful "sword" hanging over directors and senior officers.

Liquidation following non-payment of AML/CFT Penalties

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

—

Time limit for prosecuting AML/CFT offences

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?

BIG's Response

The "standard" seven-year limit for records seems a more sensible cut-off?

PART 4: Preventative measures

Customer due diligence

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

BIG's Response

Key challenges are:

1. Timing
2. Meaninglessness
3. Customer inconvenience/access to products, and
4. Complexity.

We expand on these points in answering the questions that follow.

In general terms, however, we note two illustrative challenges:

1. Whereas for a New Zealand individual with a settled and readily provable address and current identity documentation the processes tend to work satisfactorily, that is not the case for new emigrants. For such customers PEP screening especially can be problematic because there can be hundreds of people with the same foreign name. Further, their details (which are easy to validate for long-term New Zealand residents and citizens) cannot be found in common databases. Some MIS managers have settled on having no, or very few, new emigrants because these are too difficult to verify.
2. Proof of address is frequently a problem for people who lead more mobile lives and who do not pay bills for some particular reason.

For corporate entities:

- Many of the more complex entities to work through the process are high trust entities like Māori Trusts (with hundreds of trustees and thousands of beneficiaries, yet you know source of funds from the outset), community trusts and organisations like the AA.
- Family trusts are automatically treated as high risk, whereas in the NZ context, are a fairly standard family protection mechanism for a large number of New Zealanders.
- For trusts and partnerships, again collecting information about trustees is often much harder than source of funds.

In general terms, our members have a view that their CDD efforts go beyond what is necessary considering the risk profile of the typical customer we onboard. This is exacerbated by the inflexibility of the current regime. We want a regime where we commit our compliance resources to those customers that are truly riskier, and largely spare those who are not from mechanical, uniform, compliance burdens.

Definition of a customer

4.2 Have you experienced any situations where trying to identify the customer can be challenging or not straightforward? What were those situations and why was it challenging?

4.3 Would a more prescriptive approach to the definition of a customer be helpful? For example, should we issue regulations to define who the customer is in various circumstances and when various services are provided?

4.4 If so, what are the situations where more prescription is required to define the customer?

4.5 Do you anticipate that there would be any benefits or additional challenges from a more prescriptive approach being taken?

BIG's Response

CDD on customers other than natural persons is commonly time-consuming and complex. Most people, even with flowcharts/guides, still struggle to determine all the persons who require CDD under the current regime, necessitating assistance from AML Compliance staff.

A more prescriptive approach may help a bit, but what would help much more is being able to conduct CDD on fewer people when the customer is not a natural person. For example, why not demand CDD from only one of the trustees? Until any suspicion is formed, there is little value in the time expended on any CDD. Let the mandatory enhanced CDD (at the point of filing a SAR) determine when comprehensive CDD is required. Such an approach would be consistent with the aim to reduce compliance costs, reduce burden on customers, and would not increase *actual* laundering.

In principle, for many entities, especially where they do not have a direct or intimate relationship with their customers (examples: (1) mass market KiwiSaver Schemes; and (2) Wrap platforms where the client is intermediated), CDD is meaningless insofar as the purported aim being to help identifying what activities or transactions are suspicious. For many entities, CDD is simply exaggerated verification of identity, which, in and of itself does almost nothing to prevent laundering and adds significantly to compliance costs.

Some specific challenges for MIS Managers

When MIS Managers deal with platforms and some financial advice businesses it can be difficult to determine whether they have any relationship with the end customer. If they do, they may not have visibility as to who their customers are. However, this is not necessarily a problem if the MIS manager has confidence that the platform itself is undertaking the customer due diligence, either by way of an agency arrangement or preferably under a managing intermediary exemption.

This emphasises the importance within the financial sector of being of being able to rely on other businesses in situations where multiple parties are providing services to end customers at the same time in respect of the same transaction.

Definition of a customer in real estate transactions

4.6. Should we amend the existing regulations to require real estate agents to conduct CDD on both the purchaser and vendor?

4.7. What challenges do you anticipate would occur if this was required? How might these be addressed? What do you estimate would be the costs of the change?

4.8. When is the appropriate time for CDD on the vendor and purchaser to be conducted in real estate transactions?

When CDD must be conducted

4.9 Are the prescribed points where CDD must be conducted clear and appropriate? If not, how could we improve them?

BIG's Response

The biggest improvement would be to:

EITHER
Extend the time frame within which CDD must be completed for natural persons to at the time of *first withdrawal*. That requirement already exists for employer-facilitated Superannuation Scheme customers (under reg 20 of the Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011). There is no reason not to extend it wider. We consider it could be extended to all natural person customers *except* where the product/sector is rated as high or medium-high risk as defined in a Sector Risk Assessment or the National Risk Assessment.

AND / OR
Reduce the CDD requirement for low or medium-low risk customers in low or medium-low risk products, as identified in a reporting entity's Risk Assessment, to be *Simplified CDD* only. The additional information required for Standard CDD is [physical] address. In 2021 "address" is a more nebulous concept; indeed, in some cases we have to make exceptions where the customer has no physical address. So, we consider that it would be optimal to either to do away with address for the majority of clients (preferred, so go to Simplified CDD only) or, otherwise, require any form of contact details, consistent with a 2020s economy. That would mean allowing an email address, mobile phone number, or any other form of contact detail providing a means of communicating with the customer, and which can be validated back to them as 'valid' — e.g., by proof such as a verified RealMe account.

4.10 For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear?

BIG's Response

It may be helpful to provide some framing to what "unusual or complex transactions" actually encompasses but only provided any guidance is simple and not one-size-fits-all.
In particular, we would not want to see "unusual or complex transactions" get defined as something "unusual or complex" for a reporting entity versus its "usual and simple" transactions. That is because you would automatically capture transactions that are not necessarily unusual or complex per se from a risk-based perspective. Care needs to be taken not to inadvertently place burdens on reporting entities.

Dealing with trusts would be a good example of a situation whereby the law arbitrarily treats a very common structure in this jurisdiction as being of intrinsically higher risk than other structures, when it isn't.

As noted above, the regime should operate on both reporting entities and their customers in a way that is neutral as to the legal structure of the entity per se and should instead be based on an assessment of real-world risk. Returning to a thematic example, a Māori Trust that holds $20m of assets and which is known to have received a Treaty of Waitangi Settlement from the Crown for $20m should be considered low risk. The fact that the money happens to be held in a trust structure as opposed to any other structure, does not make it a riskier customer than a high net worth individual with $20m in assets but for whom you manage only a small fraction of their funds.

When we think about corporate structure it should be less along the lines of "companies are good" or "trusts are bad" and more along the lines of, "Can I easily get comfort that this entity is legitimate?" Does the entity's structure make sense or is it particularly complicated for no obvious reason?

Conducting customer due diligence in all suspicious circumstances

4.11 Should CDD be required in all instances where suspicions arise?

4.12 If so, what level of CDD should be required, and what should be the requirements regarding verification? Is there any information that businesses should not need to obtain or verify?

4.13 How can we ensure that this obligation does not put businesses in a position where they are likely to tip off the person?

BIG's Response

Provided it is offset by reduction of CDD effort on the bulk of customers who are low/medium-low risk, as we recommend above in our response to 4.9, such reporting would be fine and would also be consistent with the aim to *prevent* laundering (rather than increasing compliance and administration burdens to entities and their customers through more universal requirements). This would be a fair and appropriate trade-off.

Tipping off, when asking for enhanced CDD, is a *Catch 22*. Anyone who is *actually laundering / financing terrorism* will be tipped off if you ask for information that is exceptional. From a policy perspective, this needs to be addressed because it causes needless stress for reporting entities' staff today. Demanding enhanced CDD without a strong likelihood that the customer "smells a rat" is unrealistic. So MoJ needs decide which is more important and change the requirement to be a more objective one. That is, ***either*** require enhanced CDD and require the reporting entity not to *overtly* tip off a customer ***or*** allow the reporting entity to make a judgment call whether there is a need to conduct enhanced CDD in parallel with submitting an SAR because in some instances it is pointless (e.g., if enhanced CDD was already recently completed).

Managing funds in trust accounts

4.14 What money laundering risks are you seeing in relation to law firm trust accounts?

4.15 Are there any specific AML/CFT requirements or controls that could be put in place to mitigate the risks? If so, what types of circumstances or transactions should they apply to and what should the AML/CFT requirements be?

4.16 Should this only apply to law firm trust accounts or to any DNFBP that holds funds in its trust account?

4.17 What do you estimate would be the costs of any additional controls you have identified?

What information needs to be obtained and verified

4.18 Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?

4.19 Are the obligations to obtain and verify information clear?

4.20 Is the information that businesses should obtain and verify about their customers still appropriate?

4.21 Is there any other information that the Act should require businesses to obtain or verify as part of CDD to better identify and manage a customer's risks?

BIG's Response

This, if a truly risk-based pragmatic approach is applied, provides a huge opportunity to more appropriately resource preventing ML and FT versus adding compliance burden, inconvenience, and undue restraints to law-abiding New Zealanders. As suggested in several places already, we recommend:

1. Low and medium-low rated sectors/sub-sectors (per the NRA or Supervisors' SRAs), where the potential/actual customer is low or medium-low risk (as determined by the entity's Risk Assessment), should only require Simplified CDD.
2. The timeframe for completion of CDD should be adjusted to at first withdrawal.[6] (*By definition, there is no ML or FT risk until funds have been withdrawn, so this is consistent with a risk-based approach*).
3. The requirements to conduct ongoing CDD, especially if our recommendations regarding Simplified CDD are not taken up, need to be reviewed. We recommend that for low and medium-low rated products (per the NRA or Supervisors' SRAs) where the potential/actual customer is low or medium-low risk (as determined by the entity's Risk Assessment) there is no value in doing any ongoing CDD. The customer's name has rarely changed, and their date of birth similarly has not changed. Updated ID documents add little value because we already know the customer has been verified against an official source. And "address", which would not be required under Simplified CDD (and we expect "address" will be dropped as a requirement).

In some instances, source of funds/wealth may be easier to verify than the identities of all potentially relevant people within an organisation, with the Māori Trust example (refer our answer to 4.10) above illustrating this. We consider there is too much emphasis on CDD (and often just VOI), which serves little purpose in many cases, and a better approach would be to provide reporting entities the discretion to adjust their approach to gaining reasonable comfort that the entity they are dealing with is not engaging in ML/FT activities.

Finally, in terms of the level of verification required, there is an opportunity to reduce the burden in lower risk situations. Simplified CDD for lower risk entities/products/customers could be completed with unverified documents (e.g., provided as digital files directly to the reporting entity), for example. The need for a staff member or trusted referee today wastes a huge amount of time for customers and our members.

Obligations for legal persons and legal arrangements

4.22 Should we issue regulations to require businesses to obtain and verify information about a legal person or legal arrangement's form and proof of existence, ownership and control structure, and powers that bind and regulate? Why?

4.23 Do you already obtain some or all of this information, even though it is not explicitly required? If so, what information do you already obtain and why?

4.24 What do you estimate would be the impact on your compliance costs for your business if regulations explicitly required this information to be obtained and verified?

BIG's Response

Two of the biggest sources of work and cost, with little in the way of ML/FT risk reduction are:

1. The amount of time and effort spent gathering documentation from high trust corporate entities, as discussed in out answer to 4.10, above, and
2. Having to treat relatively simple family trusts as high risk, when they are not

[6] This is especially important because not all customers arrive by direct sign-up with a reporting entity. For example, a "book" of customers may be acquired by one entity from another reporting entity and the purchaser may find that the CDD on the customer base was patchy. Nonetheless, under today's requirements, Standard CDD is required on the lot. This is nonsensical, adds compliance costs needlessly, annoys customers who have no understanding of why needless CDD is being conducted, and generally distracts the entity from actual work on preventing ML and FT. It is even more ridiculous in circumstances where the acquired customers are "locked in" for many more years before being allowed to withdraw any funds, which is the case for superannuation schemes.

Legal form and governance of an entity is generally an important question to understand for commercial reasons. However, how far you should go verifying the identity for *every* person in a governance structure, and how far you need to go to prove it exists, is an important policy question because it is costing New Zealand hugely in compliance costs.

For example, if your customer is the Cancer Society, it is reasonable to accept that it exists, it is reasonable to gain some sort of verification from the staff that you would be dealing with, and potentially two directors / executives who might be authorising the relationship, but over and above that, collection of more information add less and less value from an AML/CFT perspective and simply adds unnecessary compliance cost to the reporting entity and similarly to the customer.

In specific response to question 4.24, we would be very concerned if requirements were increased from their current settings. They are already compliance heavy. A shift of resource allocation away from perfunctory, universal, onerous requirements should be a clear aim of the changes being formulated for the new regime. It is important to keep in mind that the clear majority of "legal persons", just like natural persons, are law-abiding. Adding even more mandatory administration wastes reporting entities' and those legal persons customers' time.

Any sort of requirement to verify "the ownership and control structure and powers that bind and regulate the person or arrangement" is going too far. This would add significant cost and effort to our onboarding arrangements and frustration for customers (the majority of whom would find such questions illogical). Collecting information in itself is frustrating; having to verify it would be really difficult and inefficient.

The government could assist by creating a register of sorts for trusts with necessary information included, saving re-work by reporting entities checking the same customers. To push this onto reporting entities and then not provide a source to verify such information would be extraordinary.

Source of wealth versus source of funds

4.25 Should we issue regulations to prescribe when information about a customer's source of wealth should be obtained and verified versus source of funds? If so, what should the requirements be for businesses?

4.26 Are there any instances where businesses should not be required to obtain this information? Are there any circumstances when source of funds and source of wealth should be obtained and verified?

4.27 Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds?

BIG's Response

Source of wealth/funds is one of the most illogical parts of the regime. When the clear majority of your customers are family trusts and individuals in superannuation schemes, asking for source of funds commonly gets meaningless (yet accurate) answers like "savings" or "salary".
We consider the requirement for demanding source of funds should be narrowed so that, for low or medium-low risk products (per the NRA/applicable SRA), and where the customer is not high risk (per the reporting entity's Risk Assessment), the source of funds requirement should no longer be required.

As it stands, it is a perfunctory requirement anyway. An example to illustrate:

A large sum is deposited, and "source of funds" is requested. The customer provides a real estate sale and purchase agreement. Is source of funds now proven? Notionally, "yes". But who is to know where the funds that bought the real estate came from?

Our point is source of funds/wealth should only be required in instances where it makes sense to request it. An example of when it is appropriate is when a potential suspicious

activity is identified. This is because at that point source of funds information may add value insofar as the suspicion will either be eliminated/reduced or increased depending on the answer. The default setting currently, much like a lot of the regime, is "one size fits all". A risk-based redesign, focused on preventing ML/FT rather than adding universal compliance cost, is needed.

Beneficiaries of life and other investment-related insurance

4.28 Should we issue regulations to require businesses to obtain information about the beneficiary/ies of a life insurance or investment related insurance policy and prescribe the beneficiary/ies as a relevant risk factor when determining the appropriate level of CDD to conduct? Why or why not?

4.29 If we required this approach to be taken regarding beneficiaries of life and other investment-related insurance policies, should the obligations only apply for moderate or high-risk insurance policies? Are there any other steps we could take to ensure compliance costs are proportionate to risks?

Identifying the beneficial owner

Definition of beneficial owner

4.30 Have you encountered issues with the definition of a beneficial owner? If so, what about the definition was unclear or problematic?

4.31 How can we improve the definition in the Act as well as in guidance to address those challenges?

BIG's Response

The main challenge with Beneficial Owner, Beneficiary, Acting on Behalf, etc., is that laypeople struggle to understand requirements and similar sounding terms. This makes it challenging for reporting entities. For example, when dealing with intermediaries (who despite often being reporting entities themselves), they commonly have little idea what they need to do. There is opportunity to: (a) reduce jargon, (b) provide better, simple, guidance, and (c) articulate why/what risk is being prevented by demanding this information from *every* customer (i.e., rather than only when a suspicion is raised).

4.32 Should we issue a regulation which states that businesses should be focusing on identifying the 'ultimate' beneficial owner? If so, how could "ultimate" beneficial owner be defined?

BIG's Response

No. The regime is too complicated already and over-prescriptive. It does not need more rigidity. If this did become a focus, it should only apply to high-risk products where the customer is also assessed as high risk. Control is a nuanced thing. Do we stop at the directors of the customer we are onboarding (if they are not nominee directors) or continue to directors of the holding company? We feel that there is a limit to what is reasonable and, again, risk should drive these decisions, not a rigid requirement/focus as it will be different depending on the circumstances.

Also, as noted above, the financial sector often involves institutions investing in other institutions to ultimately serve an end customer. It is an important concept that only the institution with the end customer facing relationship needs to carry out AML/CFT checks on the ultimate end customer and then have the other institutions rely on the first institution. Otherwise if XYZ Bank invested money with one of our members as part of its KiwiSaver scheme, the member would have to try to look through to all the end customers who invested with XYZ Bank and the financial system would break down.

4.33 To extent are you focusing beneficial ownership checks on the 'ultimate' beneficial owner, even though it is not strictly required?

4.34 Would there be any additional costs resulting from prescribing that businesses should focus on the 'ultimate' beneficial owner?

BIG's Response

See comment above about the intrinsic need for financial sector institutions to be able to rely on other institutions. In addition, we already attempt to get to the ultimate owner when we come across highly complex, deep structures. Thankfully that is not that common for us, but when it does happen it is *very* resource intensive and often confusing for the people who information is being requested from (because they just don't get it). As suggested, this needs to be restricted to high-risk customers/products because otherwise it is a "sledgehammer to crack a walnut".

4.35 Should we issue a regulation which states that for the purposes of the definition of beneficial owner, a person on whose behalf a transaction is conducted is restricted to a person with indirect ownership or control of the customer (to align with the FATF standards)? Why or why not?

BIG's Response

Yes, because it is conceptually easier to understand and also, if the customer is engaging in some form of ML or FT activity, it will not be driven by persons with no ability to influence its activities.

4.36 Would this change make the "specified managing intermediaries" exemption or Regulation 24 of the AML/CFT (Exemption) Regulations 2011 unnecessary? If so, should the exemptions be revoked?

BIG's Response

The change would remove the problem of having to carry out AML/CFT checks on thousands of individual underlying customers, which would be an impossibility. However, the exemption would still be valuable in many situations. For example, if there is a FMCA Supervisor standing between a complex institutional customer and a fund manager that it is investing in, it would remove a lot of unnecessary work if the fund manager can rely on checks already carried out by the Supervisor. (Potentially if an institutional client has a New Zealand statutory supervisor such as Public Trust overseeing its activities that is a good indicator that it is a highly regulated high trust entity in itself).

Broadening the Simplified CDD requirements to all those currently classified as LMIs would, given LMIs and Simplified requirements are almost exactly the same, would simplify things.

4.37 Would there be any additional compliance costs or other consequences for your business from this change? If so, what steps could be taken to minimise theses costs or other consequences?

BIG's Response

Yes, there would be significant additional work onboarding high trust institutional clients for the reasons given above. A way to remedy this would be to have a more extensive list of customers eligible to be subject to simplified due diligence only (or, indeed, exempt from CDD altogether). Examples are:

1. In the case of the financial sector, any entity that has a statutory supervisor or that holds an FMC Act market services licence should be as high a trust entity as a listed entity.
2. Any entity that has to go through some form of rigorous licensing process with a New Zealand Government agency that involves proving its bona fides.
3. Entities long established via some form of Government or quasi government process: Māori Trusts, community trusts, very high trust charities or organisations like Auckland City Mission, Cancer Society, the AA, Starship, etc.

4. Any Court-appointed entity, when acting in its appointed capacity.

Process for identifying who ultimately owns or controls legal persons

4.38 What process do you currently follow to identify who ultimately owns or controls a legal person, and to what extent is it consistent with the process set out in the FATF standards?

4.39 Should we issue regulations or a Code of Practice which is consistent with the FATF standards for identifying the beneficial owner of a legal person?

4.40 Are there any aspects of the process the FATF has identified that not appropriate for New Zealand businesses?

4.41 Would there be an impact on your compliance costs by mandating this process? If so, what would be the impact?

BIG's Response

This is not usually a big issue for us because there are not that many entities which are so complex that such a Code of Practice would help and, in general, we are reluctant to support more Codes, especially if the result was more inflexible universal compliance requirements that are not risk based.

Process for identifying who ultimately owns or controls legal arrangements

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

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

BIG's Response

The requirements for Trusts are already extensive and burdensome for all involved. It would be foolish to add even more people into the mix requiring identification. Either the status quo should stand or, preferably, the prevailing requirements be simplified and made more risk-based when the trust is not high risk. (E.g. a basic New Zealand-based family trust with "mum and dad" and a corporate trustee as trustees should have lesser requirements.)

Reasonable steps to verify information obtained through CDD

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

BIG's Response

No, they are not appropriate currently. Please refer to the myriad answers throughout this submission illustrating how, frequently, they are unnecessarily burdensome.

Identity Verification Code of Practice

4.45 Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?

4.46 Is the approach in IVCOP clear and appropriate? If not, why?

4.47 Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g verifying name and date of birth of high risk customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?

4.48 Are there any identity documents or other forms of identity verification that businesses should be able to use to verify a customer's identity?

4.49 Do you have any challenges in complying with Part 3 of IVCOP in relation to electronic verification? What are those challenges and how could we address them?

BIG's Response

There is certainly irony in mandating CDD requirements for lower risk customers via the IVCOP yet leaving reporting entities to work it out for themselves for higher risk customers. In that context, the IVCOP is unhelpful help.

As outlined throughout this submission, there is far too much emphasis on CDD and not enough on suspicious activity identification.[7] There is no laundering prevention unless it is identified, and CDD does not (for many entities where the "relationship" with customers is not really a relationship at all) do much other than add compliance cost and customer inconvenience.

The best means of smoothing the IVCOP process would be to provide direct access to official sources to validate data and documents. The current processes, which require third parties to do this, are inefficient. The IVCOP has, until biometric capabilities caught up only recently, been fairly useless given the requirement to verify that the person presenting is *actually* the customer.

Ideally, any form of government-issued identification should be allowed. This should extend into common overseas governments' documents too, especially those most commonly encountered (i.e., Australia, but also whatever "top 5" countries are identified as most common in annual reporting to the Supervisors, which we expect would then include the UK and a few other low-risk jurisdictions, as rated by FATF).

The IVCOP itself has been too inflexible, and quickly outdates/is not easily updated/adapted. It has inhibited innovation and is a classic one-size-fits-all approach to compliance with CDD. Our preference is that it is discarded or overhauled entirely. The Act requires verification according to a reliable and independent source, which is sufficient at the top end, and could be potentially loosened even further for low-risk customers/products where such independence is not really necessary.

[7] To illustrate, there were only three (**3**) SARs by the entire Financial Advisers sector identified in the FMA's 2017 Sector Risk Assessment. That seems implausibly low given the huge number of customers being serviced by that sector. However, that sector would have completed tens of thousands of hours over the same measurement period doing CDD-related activity.

Verifying the address of customers who are natural persons

4.50 What challenges have you faced with verification of address information? What have been the impacts of those challenges?

4.51 In your view, when should address information be verified, and should that verification occur?

4.52 How could we address challenges with address verification while also ensuring law enforcement outcomes are not undermined? Are there any fixes we could make in the short term?

BIG's Response

Physical address verification is an archaic requirement. Many customers nowadays could not care less about providing their physical address because they conduct their affairs electronically. Consistent with other jurisdictions, as noted, the requirement for address verification should be removed. It adds little/no value, adds compliance cost, and is an impediment to potential customers accessing financial services/products.[8]

All address requirements should be eliminated with the *possible* exception of when enhanced CDD is conducted in relation to a SAR filing (and only then if there isn't a relatively recently determined address). At *that point* the physical address of a customer *may* be relevant for law enforcement.[9] This would be a much better approach, risk-based, right-sized, and helpful.

Obligations in situations of higher and lower risk

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

4.53 Do you currently take any of the steps identified by the FATF standards to manage high-risk customers, transactions or activities? If so, what steps do you take and why?

4.54 Should we issue regulations or a Code of Practice which outlines the additional measures that businesses can take as part of enhanced CDD?

4.55 Should any of the additional measures be mandatory? If so, how should they be mandated, and in what circumstances?

BIG's Response

Some steps our members take include: "watch listing" potentially suspicious customers and looking at all transactions; some members also demand that all payments only be made to the account in the customer's name, which is a key risk control reducing the likelihood of fraud; and seeking additional information, especially from intermediary financial advisers when there are suspicions is another common practice.

A lot of care should be taken not to make this suggestion mandatory, i.e., "obtaining the approval of senior management to commence or continue the business relationship". Although it sounds sensible in theory, many of our customers have an unalienable right to use our products once they are members. An example is KiwiSaver Schemes: we cannot just decide we do not want to continue a business relationship even if the client is obviously suspicious or, indeed, even admitted criminal activities. Indeed, drug crime is the largest source of ML in New Zealand (as noted in recent reporting) and we identify, via screening,

[8] Incidentally, it is not only AML/CFT regulations where such requirements should be modified. Another clear example is Managed Investment Schemes: requirements should adjust to the 21st Century and consider "address" as a variable thing, determined based on customer preference. If the customer provides a verified email address that is far more valuable today than a physical address.

[9] For law enforcement to suggest that their outcomes are undermined by reporting entities not verifying this information for *all* customers must be backed up by hard facts and data. We content there is no conceivable reason that addresses should be required for all customers for any legitimate law enforcement purposes. Only once a potential offence has been determined to be worthy of investigation should the requirement to gather a physical address be necessary.

scores of customers every year who have been convicted of such crimes (flagged in some screening tools as "Persons of Interest" or similar designations), but we cannot cease such customers' memberships even if we did decide we did not want to continue doing business with them.

In particular, care must be taken to ensure any requirements/additional measures are truly only mandated for high-risk customers.

Conducting simplified CDD on persons acting on behalf of large organisations

4.56 Are there ways we can enhance or streamline the operation of the simplified CDD obligations, in particular where the customer is a large organisation?

4.57 Should we issue regulations to allow employees to be delegated by a senior manager without triggering CDD in each circumstance? Why?

BIG's Response

Large entities such as Trustee corporations, NZX listed entities and Court-appointed administrators are all examples of where requiring CDD is meaningless (and there are many more examples that could be provided).

Likewise, certain licensees (MIS managers especially) are also examples of where demands for CDD are about form rather than substance. We consider that there is scope for exemptions to conduct any CDD on such entities. If this was considered a step too far, we suggest that a centralised "CDD repository" could be maintained for this group of "customers" enabling any reporting entity to access when they receive a new business relationship request. That would provide massive efficiencies because the number of times some entities have been CDDed must be in the hundreds, with no conceivable improvement in New Zealand's AML/CFT outcomes, and certainly with lots of wasted compliance effort/costs mounting with every request.

Mandatory enhanced CDD for all trusts

4.58 Should we remove the requirement for enhanced CDD to be conducted for all trusts or vehicles for holding personal assets? Why or why not?

4.59 If we removed this requirement, what further guidance would need to be provided to enable businesses to appropriately identify high risks trusts and conduct enhanced CDD?

BIG's Response

In New Zealand a trust is a very common structure that many ordinary people use, whereas in other FATF jurisdictions presence of a trust may be quite out of the ordinary and used in more complex activities, which may point to a cultural difference at play.

Our principled point is that choice of corporate vehicle is not in itself determinative of risk. Whether it be a trust, a company, a partnership or something else, what we should be thinking about is more along the lines of, "Do I know who this entity is?", "How well do I know the entity?", "Do I understand what it does?", "Does the structure make sense?", "Would this entity have to go through some licensing process that establishes its bona fides?", etc., rather than automatically ascribing risk based on legal form.

Consequently, we advocate a more risk-based approach to CDD on trusts. Only trusts that have been identified as medium-high / high risk should be subject to enhanced CDD. For example, a foreign trust with trustees from low-rated FATF jurisdictions is a different profile to the clear majority of trusts that our reporting entities deal with — i.e. New Zealand-

residents' family trusts.[10] The ML/FT risk posed by the latter does not warrant enhanced CDD. A risk-based approach would support removal of universal, mandatory, enhanced CDD on trusts.

In conclusion, we support recognising that not all trusts are high risk. Explaining characteristics of high-risk categories of trusts would be welcome, and we would welcome industry engagement on such guidance.

4.60 Should high-risk categories of trusts which require enhanced CDD be identified in regulation or legislation? If so, what sorts of trusts would fall into this category?

BIG's Response

See answer above, that considering things on the basis of pure legal structure is probably the wrong approach, and instead it should be more a case of asking questions like the ones articulated in that answer.

It may be possible to achieve either a high level of comfort or a high level of discomfort in some instances without having to take the analysis too far. For example, if it quickly becomes apparent that the entity was established by the public sector in its past and that assets belong to the community, you will get comfort very quickly. Conversely if you gain a sense that funds are coming from certain overseas jurisdictions you may get discomfort very quickly.

Ongoing customer due diligence and account monitoring

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

BIG's Response

Change so that it is only mandatory to actively conduct ongoing CDD for high risk or medium-high risk customers with high risk or medium-high risk products. The clear majority of ongoing CDD is superfluous in terms of prevention or deterring ML/FT. For example, for superannuation scheme products, the nature and purpose of the product is self-evident, and the details of the customers rarely change (especially when, as we expect, physical address is removed as a requirement), hence the only data point that could change is a person's name though marriage or deed poll, which is relatively rare.

Considering whether and when customer due diligence was last conducted

4.62 As part of ongoing CDD and account monitoring, do you consider whether and when CDD was last conducted and the adequacy of the information previously obtained?

4.63 Should we issue regulations to require businesses to consider these factors when conducting ongoing CDD and account monitoring? Why?

4.64 What would be the impact on your compliance costs if we issued regulations to make this change? Would ongoing CDD be triggered more often?

4.65 Should we mandate any other requirements for ongoing CDD, e.g. frequently it needs to be conducted?

BIG's Response

There should be no need to issue any regulations providing the triggers for ongoing CDD are significantly refined, as suggested. Again, we recommend that ongoing CDD should only be mandatory for high risk or medium-high risk customers using high risk or medium-high risk

[10] The following features would indicate that a trust is NOT high risk: *(a)* A trust deed that is relatively simple, governed by NZ law, has a clear link to NZ, and all trustees reside in NZ or Australia; *(b)* One or more trustees are also beneficiaries of the trust, *(c)* Settlors/appointors reside in NZ; *(d)* No PEPs or other persons of interest involved; *(e)* a NZ bank account.

products. Such customers should be continually CDDed anyway, though the frequency could be subject to guidance as to what is appropriate for different product-customer-jurisdiction-method combinations to distinguish best practice frequencies and so forth.

Ongoing CDD requirements where there are no financial transactions

4.66 If you are a DNFBP, how do you currently approach your ongoing CDD and account monitoring obligations where there are few or no financial transactions?

4.67 Should we issue regulations to require businesses to review activities provided to the customer as well as account activity and transaction behaviour? What reviews would you consider to be appropriate?

4.68 What would be the impact on your compliance costs if we issued regulations to make this change?

Information that needs to be reviewed for account monitoring

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

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

BIG's Response

We review activities and then also inquire of intermediaries in many instances. No additional mandatory requirements should be added, though it could be useful to have additional guidance. Even more useful, however, would be regular typologies being published. Actual identified ML and FT exemplars are always more useful than more theoretically focused guidance.

There seems to have been less typology content recently and the publicity/promotion around what has been published historically is limited, which makes us consider that many reporting entities are unaware of its existence.

We do not consider more rules / regulations would help. There are more than enough rules now and we fear more regulations would add more to compliance costs than they would to ML/FT deterrence, detection or prevention.

Finally, some suggestions regarding additional monitoring, e.g., of a customer's IP address is both excessive and impracticable. It is very simple to use a VPN or Tor to avoid IP address detection, so this would be pointless.

Conducting CDD on existing (pre-Act) customers

Making the trigger an 'or' rather than an 'and'
Changing what is meant by a 'material change'

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

BIG's Response

Pre-Act customers, where they are in low or medium-low risk AML products (per the applicable Sector Risk Assessment), should not have any mandatory CDD introduced. This is another example of where a risk-based approach is needed.

Completion of CDD for the clear majority of customers does almost nothing to prevent ML/FT because 99%+ of them are bona fide citizens and residents. Only where risk factors point to value in CDD being completed should it be necessary for pre-Act customers, for

example, when a Suspicious Activity Report is lodged in relation to the customer, or perhaps, if the customer's address changed to a poorly rated (by FATF) country.

Having reporting entities do more on existing customers does not reflect the risk that these customers have. What it would do is create more compliance "remediation" work, which drives up cost and directs resources away from where true risk really resides.

Avoiding tipping off

4.72 Should the Act set out what can constitute tipping off and set out a test for businesses to apply to determine whether conducting CDD or enhanced CDD may tip off a customer?

4.73 Once suspicion has been formed, should reporting entities have the discretion not to conduct enhanced CDD to avoid tipping off?

4.74 If so, in what circumstances should this apply? For example, should it apply only to business relationships (rather than occasional transactions or activities)? Or should it only apply to certain types of business relationships where the customer holds a facility for the customer (such as a bank account)?

4.75 Are there any other challenges with the existing requirements to conduct enhanced CDD as soon as practicable after becoming aware that a SAR must be reported? How could we address those challenges?

BIG's Response

This is one of the most perverse areas of the prevailing regime. The current requirement to conduct ongoing enhanced CDD (after being aware that a SAR will be reported) is highly likely to be suspicious itself to a customer, so it's *de facto* tipping off.

The simple policy priority needs to be *one of*, not *both*, of:

Conducting enhanced CDD on reported-to-FIU customers

OR

Not tipping off customers who are reported to FIU

Expecting both is wanting to have your cake and eat it too. Worse, it adds stress to staff who are already struggling to get enhanced CDD completed for such customers, especially if challenged as to why they are being asked for such information. Either the staffer lies, or they tip off the customer. This creates needless stress for staff.

Our view is that requiring enhanced CDD in such circumstances should be optional *except* where no CDD has already been completed for such a customer due to, for example, pre-dating the AML regime. For such customers, the staff explanation is straightforward – i.e., that the customer has never been CDDed before and that the reporting entity is just doing routine catch-up, which would be a lie, but is at least a plausible story.

In our view, the priority should be actually submitting the SAR, not doing an (or another) enhanced CDD request.

Another option could be for: *(a)* CDD to only be required if FIU explicitly requested that the reporting entity do it (because FIU was interested in progressing the case), but *(b)* for a relief to apply to the reporting entity that it could request the enhanced CDD from the customer without concern about, if the customer was effectively tipped off, that the reporting entity would be penalised (except where they explicitly divulged that FIU had requested the enhanced CDD be completed).

What should not be done is have a complex process by which staff/entities have to evaluate whether they will tip off customers. That is more administration and would *add* compliance cost, so that should definitely not be progressed.

As noted above, it may also be appropriate to continue with processing a transaction provided the assets do not leave control of New Zealand reporting entities, for the same reasons.

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?

BIG's Response

The biggest challenge with record keeping is navigating the competing, and at times conflicting, requirements of different legislation, including FMCA (and the Standard Conditions of the many licences that fall under it) and the Privacy Act.

It is a pity that there is not a standalone *Mandatory Record Keeping and Disposal Act 202x* consolidating the myriad legislative and regulatory requirements into a coherent whole. The inefficiency and complexity of record keeping requirements disparately spread across so much primary, secondary and tertiary legislation is further amplified when reporting entities' policies (and, for some, group record-keeping Policies also) are factored.

The simple answer is that it would be far more efficient, and reflect reality, if there was more ability to retain records almost indefinitely where there is any likelihood of it serving a law enforcement purpose. The danger/detriment to customers or ex-customers of entities retaining data is relatively low, provided it is stored securely, so there is lots of opportunity to simplify this area, from a policy perspective, which would deliver significant compliance cost reductions for reporting entities.

The current expectations around record disposal are aspirational and/or unrealistic in a 21st Century context. That is because data, once created, is almost impossible to entirely expunge – backups and versioning are ubiquitous and inherent features of modern software and SaaS offerings, so expecting record removal is simply unrealistic.

Transactions outside a business relationship

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?

BIG's Response

New Zealand, to some extent, relies on businesses being able to carry out activities that fall outside of their usual operations because our markets can be so small that there may not be an easy alternative for customers.

This is an example of New Zealand being in a different position to many other jurisdictions as a result of its small scale.

If there is no relief, those quality-of-life transactions will cease.

Politically Exposed Persons

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

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

BIG's Response

For low-risk entities (per the NRA and applicable SRA) dealing with predominantly New Zealand citizens and permanent residents, the PEP regime is a huge compliance cost that delivers no value. To illustrate, in over eight years, we have members who have not identified any PEPs whatsoever despite using industry leading screening services.

The cost of the screening cloud software is considerable. As one of our members notes, it has expended well over $100,000 since the AML/CFT regime commenced. And that did not include the staff cost of reviewing potential PEPs identified via screening, noting there are huge numbers of "false positives" that need review by Compliance staff.

The absurdity is even more stark: for the clear majority of most of B.I.G.'s entities' customers the product rules (legislated for superannuation schemes) prevent cessation of the business relationship even if/when a PEP is identified. So the requirement to review and determine whether to *cease the business relationship* is redundant. For the remaining customers (i.e., in products where the relationship *could* be ended), unless there was a particularly egregious PEP relationship it is likely to persist even after review.

The solution to this is to not require PEP screening for customers where the product provides an overriding unalienable right to remain a member (i.e., where there is no ability to unilaterally cease the business relationship).

Definition of a politically exposed person

4.81 How do you currently treat customers who are domestic PEPs or PEPs from international organisations?

4.82 Should the definition of 'politically exposed persons' be expanded to include domestic PEPs and/or PEPs from international organisations? If so, what should the definitions be?

4.83 If we included domestic PEPs, should we also include political candidates and persons who receive party donations to improve the integrity of our electoral financing regime?

4.84 What would be the cost implications of such a measure for your business or sector?

BIG's Response

"Domestic PEPs" is an oxymoron: the Act specifically excludes politically exposed persons who are New Zealanders. This makes sense and should be maintained. This is a common-sense, risk-based, approach. New Zealand is one of the least corrupt countries, as MoJ notes, so requiring local PEP screening would add compliance cost without reducing risk.

Any extension of current PEP definitions should not happen: the ML/FT reward versus compliance cost equation would be massively mis-balanced to the compliance cost side.

Time limitation of PEP definition

4.85 How do you currently treat customers who were once PEPs?

4.86 Should we require a risk-based approach to determine whether a customer who no longer occupies a public function should still nonetheless be treated as a PEP?

4.87 Would a risk-based approach to former PEPs impact compliance costs compared to the current prescriptive approach?

Identifying whether a customer is a PEP

Foreign PEPs

4.88 What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP?

BIG's Response

As noted, we have used industry-leading cloud services to seek to identify foreign PEPs but, the reality is, for us it is a worthless exercise because foreign PEPs simply do not utilise our predominate products (KiwiSaver and superannuation schemes) and their members *cannot be compulsorily exited* due to the prevalence of the legislation that provides an inalienable right to retain membership in the product.

4.89 Do you consider the Act's use of "take reasonable steps" aligns with the FATF's expectations that businesses have risk management systems in place to enable proactive steps to be taken to identify whether a customer or beneficial owner is a foreign PEP? If not, how can we make it clearer?

4.90 Should the Act clearly allow business to consider their level of exposure to foreign PEPs when determining the extent to which they need to take proactive steps?

4.91 Should the Act mandate that businesses undertake the necessary checks to determine whether the customer or beneficial owner is a foreign PEP before the relationship is established or occasional activity or transaction is conducted?

—

Domestic or international organisation PEPs

4.92 How do you currently deal with domestic PEPs or international organisation PEPs? For example, do you take risk-based measures to determine whether a customer is a domestic PEP, even though our law does not require this to be done?

4.93 If we include domestic PEPs and PEPs from international organisations within scope of the Act, should the Act allow for business to take reasonable steps, according to the level of risk involved, to determine whether a customer or beneficial owner is a domestic or international organisation PEP?

BIG's Response

"Domestic PEPs" is an oxymoron: they are not PEPs at all. We consider the status quo is appropriate for the reasons already stated.

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

BIG's Response

If our recommendation to remove KiwiSaver Schemes and superannuation products from PEP screening entirely is not adopted, the compliance cost of "domestic PEP" screening would be considerable. Some of our members have significant numbers of Members of the New Zealand Parliament as members. Their interest in superannuation schemes is already disclosed in the pecuniary interests' disclosures, so requiring senseless screening of them, especially when they could not be compulsorily exited (as already noted), would be added compliance cost for absolutely no value.

Beneficiaries of life insurance policies

4.95 Should businesses be required to take reasonable steps to determine whether the beneficiary (or beneficial owner of a beneficiary) of a life insurance policy is a PEP before any money is paid out?

4.96 What would be the cost implications of requiring life insurers to determine whether a beneficiary is a PEP?

—

Mitigating the risks of politically exposed persons

4.97 What steps do you currently take to mitigate the risks of customers who are PEPs?

4.98 Should the Act mandate businesses take the necessary mitigation steps the FATF expects for all foreign PEPs, and, if domestic or 72 PART 4 international organisation PEPs are included within scope, where they present higher risks?

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

—

BIG's Response

A novel proposal in relation to PEP screening

A huge opportunity vis-à-vis PEP screening for "NZ Inc" is to consider the centralisation of screening into a Pharmac-like model. Reporting entities have spent millions, if not tens of millions of dollars, on PEP screening using foreign-based providers of such services. This is huge inefficiency and inconsistency. It could be improved by a government entity procuring a single provider, at sharp price (due to the massive volume that would be offered), to do all of New Zealand's PEP screening. Further, if a central database was maintained whereby the same customer who had returned a negative PEP result within the last *N* months was a precursor test, screening could be set aside – in doing so, masses of *repeat* PEP screens would be avoided, saving even more.

The plain fact is, requiring individual reporting entities to conduct PEP screening is incredibly inefficient from both a cost and redundancy perspective.

This is an area that is worthy of serious consideration because the current regime delivers significant profits to the providers of these services, most of whom are overseas entities.

To cap it off, AML/CFT Supervisors expect reporting entities to evaluate the quality of the PEP screening providers that they use. This is another compliance cost that would be eliminated by an efficient, centrally procured and provided screening solution.

Implementation of targeted financial sanctions

Assessing exposure to designated individuals or entities and sanctions evasion

4.100 Should businesses be required to assess their exposure to designated individuals or entities?

4.101 What support would businesses need to conduct this assessment?

4.102 If we require businesses to assess their proliferation financing risks, what should the requirement look like? Should this assessment be restricted to the risk of sanctions evasion (in line with FATF standards) or more generally consider proliferation financing risks?

BIG's Response

We do not consider any additional requirements in this area should be extended to low or medium-low risk sectors/subsectors, consistent with an appropriate risk-based approach.

Including TFS implementation in an AML/CFT programme

4.103 Should legislation require businesses to include, as part of their AML/CFT programme, policies, procedures, and controls to implement TFS obligations without delay? How prescriptive should the requirement be?

4.104 What support would businesses need to develop such policies, procedures, and controls?

BIG's Response

We do not consider any additional requirements in this area should be extended to low or medium-low risk sectors/subsectors, consistent with an appropriate risk-based approach.

Prompt notification about designated persons and entities

4.105 How should businesses receive timely updates to sanctions lists?

4.106 Do we need to amend the Act to ensure all businesses are receiving timely updates to sanctions lists? If so, what would such an obligation look like?

4.107 How can we support and enable businesses to identify associates and persons acting on behalf of designated persons or entities?

BIG's Response

We do not consider any additional requirements in this area should be extended to low or medium-low risk sectors/subsectors, consistent with an appropriate risk-based approach.

Screening for designated persons and entities

4.108 Do you currently screen for customers and transactions involving designated persons and entities? If so, what is the process that you follow?

4.109 How could the Act support businesses to screen customers and transactions to ensure they do not involve designated persons and entities? Are any obligations or safe harbours required?

4.110 If we created obligations in the Act, how could we ensure that the obligations can be implemented efficiently and that we minimise compliance costs?

BIG's Response

Screening solutions often capture designated persons and entities as a matter of course. This is fine because it adds no compliance cost, however, consistent with our risk-based thematic, if obligations were added in relation to these, a risk-based approach would, at the most, see such obligations restricted to customers with foreign indicia (much like the system in place for the Common Reporting Standard). Ideally, however, such screening should not be mandatory for low to medium low risk sectors/subsectors.

Notification of actions taken

4.111 How can we streamline current reporting obligations and ensure there is an appropriate notification process for property frozen in compliance with regulations issued under the United Nations Act?

4.112 If we included a new reporting obligation in the Act which complies with UN and FATF requirements, how could that obligation look? How could we ensure there is no duplication of reporting requirements?

—

Providing assurance for ongoing freezing action

4.113 Should the government provide assurance to businesses that have frozen assets that the actions taken are appropriate?

4.114 If so, what could that assurance look like and how would it work?

—

BIG's Response

General response regarding Q4.100 - Q4.114

Targeted Financial Sanctions is an area that potentially would add massive compliance costs to reporting entities. This is especially so if the rules and requirements were made one-size-fits-all. And expansion of the regime needs to be proportionate to the risks involved.

More actively supervision and/or explicit requirements, such as requiring Risk Assessments and Programmes to factor lots of specific considerations, adds to complexity and, for low or

medium-low risk entities, the result would likely be increased compliance costs with no corresponding increase in identification of reporting of designated persons or entities.

Consistent with our risk-based recommendations, any extension to the current settings should only apply to high-risk sectors (per Sector Risk Assessments) and/or high risk or foreign indicia customers.

To illustrate why this would be a common-sense approach, consider one of our member's observations. For context, yes, the member does screen for customers with indicia of connection to a sanctioned country but, since the commencement of the AML/CFT regime, has had only *one* individual (a KiwiSaver) who was identified as *temporarily* resident in a sanctioned country (Iran). This illustrates the need to be circumspect and not apply blanket requirements that would add huge compliance costs but add little insofar as addressing the concern around improving designated person identification and treatment.

So, to recap, any extension of requirements in this area needs to be carefully weighed from a reward (ML/FT reduction) versus compliance cost perspective. It would be unfortunate if the result was the introduction of requirements that delivered very little reduction in ML/FT but added needless costs to lower risk entities, which inevitably flow done to their customers.

Correspondent banking

4.115 Are the requirements for managing the risks of correspondent banking relationships set out in section 29 still fit-for-purpose or do they need updating?

4.116 Are you aware of any correspondent relationships in non-banking sectors? If so, do you consider those relationships to be risky and should the requirements in section 29 also apply to those correspondent relationships?

—

Money or value transfer service providers

Maintaining a list of agents

4.117 If you are an MVTS provider which uses agents, how do you currently maintain visibility of how many agents you have?

4.118 Should a MVTS provider be required to maintain a current list of its agents as part of its AML/CFT programme?

4.119 Should a MVTS provider be explicitly required to monitor and manage its agents for compliance with its AML/CFT programme (including vetting and training obligations)?

—

Ensuring agents comply with AML/CFT obligations

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

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

4.122 Should we issue regulations to explicitly require MVTS providers to monitor and manage its agents for compliance with its AML/CFT programme (including vetting and training obligations)? Why or why not?

4.123 What would be the cost implications of requiring MVTS providers to include agents in their programmes?

—

Multiple layers to agency relationships

4.124 Who should be responsible for the AML/CFT compliance for subagents for MVTS providers which use a multi-layer approach? Should it be the MVTS provider, the master agent, or both?

4.125 Should we issue regulations to declare that master agents are reporting entities under the Act in their own right? Why or why not?

4.126 What would be the cost implications of requiring MVTS providers to include agents in their programmes?

—

New technologies

Understanding the risk of new products or technologies

4.127 What risks with new products or technologies have you identified in your business or sector? What do you currently do with those risks?

4.128 Should we issue regulations to explicitly require businesses to assess risks in relation to the development of new products, new business practices (including new delivery mechanisms), and using new or developing technologies for both new and pre-existing products? Why or why not?

4.129 If so, should the risks be assessed prior to the launch or use of any new products or technologies?

4.130 What would be the cost implications of explicitly requiring businesses to assess the risks of new products or technologies?

BIG's Response

Reviewing the ML/TF risks that new products or technology bring to our businesses is work already completed by many as part of their annual reviews of their risk assessments. Without guidance, reporting entities must determine for themselves what is appropriate. Guidance, but only if it is truly helpful and not interpreted by auditors blindly as 'rules', is important.

Existing requirements to mitigate the risks that new technology brings is sufficient. An explicit requirement to complete a risk assessment would be excessive. Any changes will already be picked up in the existing risk assessment review process. (And to complete a risk assessment to update your existing risk assessment would be nonsensical).

Mitigating the risks of new products or technologies

4.131 Should we issue regulations to explicitly require businesses to mitigate risks identified with new products or technologies? Why or why not?

4.132 Would there be any cost implications of explicitly requiring business to mitigate the risks of new products or technologies?

—

Virtual asset service provider obligations

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

—

Threshold for occasional transactions

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

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

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

—

Declaring virtual asset transfers to be wire transfers

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

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

—

Wire transfers

Terminology involved in a wire transfer

4.139 What challenges have you encountered with the definitions involved in a wire transfer, including international wire transfers?

4.140 Do the definitions need to be modernised and amended to be better reflect business practices? If so, how?

4.141 Are there any other issues with the definitions that we have not identified?

—

Ordering institutions

Wire transfers below the applicable threshold

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

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

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

—

Stopping wire transfers that lack the required information

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

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

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

—

Intermediary institutions

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

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

4.150 If you act as an intermediary institution, do you do some or all of the following:
• keep records where relevant information cannot be passed along in the domestic leg of a wire transfer where technical limitations prevent the information from being accompanied?
• take reasonable measures to identify international wire transfers lacking the required information?
• have risk-based policies in place for determining what to do with wire transfers lacking the required information?

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

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

—

Beneficiary institutions

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

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

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

—

Prescribed transaction reports

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

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

—

Types of transactions requiring reporting

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

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

—

Who is required to submit a report

Non-bank financial institutions and DNFBPs

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

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

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

BIG's Response

It would add needless compliance cost to any additional reporting entities (i.e., outside the scope of PTRs today) to be swept into the current regime. We oppose any extension to the regime because it would do little to reduce ML/FT risk (it would just create duplicate reporting which realistically nobody is likely to do anything with) whereas it would add significant compliance costs in terms of design and operationalisation for reporting entities that today are effectively outside the scope of PTR.

Intermediary institutions

4.163 Should we amend the existing regulatory exemption for intermediary institutions so that it does not apply to MVTS providers?

4.164 Are there any alternative options that we should consider which ensure that financial intelligence on international wire transfers is collected when multiple MVTS providers are involved in the transaction?

4.165 Are there any other intermediary institutions that should be included in the exemption?

—

When reports must be made

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

—

Applicable threshold for reporting prescribed transactions

4.167 Do you consider that a lower threshold for PTRs to be more in line with New Zealand's risk and context? If so, what would be the appropriate threshold for reporting?

4.168 Are there any practical issues not identified in this document that we should address before changing any PTR threshold?

4.169 How much would a change in reporting threshold impact your business?

4.170 How much time would you need to implement the change?

—

Reliance on third parties

Effectiveness of reliance provisions

4.171 Do you use any of the reliance provisions in the AML/CFT Act? If so, which provisions do you use?

4.172 Are there any barriers to you using reliance to the extent you would like to?

4.173 Are there any changes that could be made to the reliance provisions that would mean you used them more? If so, what?

BIG's Response

Some of our members do use the reliance provisions. For example, one member has: *(a)* Two reporting entities that rely on the lead reporting entity member to conduct CDD. Since they are related companies, that makes sense and is efficient, and *(b)* Reliance on dozens of reporting entities (who engage financial advisers) to complete components of CDD.

A change that we consider is worth looking into is in relation to annual reporting. There is a lot of duplication in annual reporting because individual reporting entities report their transactions. However, each transaction may channel through several reporting entities. For example, a FAP may report transactions that are reported also by the MIS the FAP's clients are invested in. This amplifies the number of reported transactions, meaning the SRAs and NRA have wildly inflated data. A partial solution would be for reporting entities to be able to indicate the *downstream* entities for which they are excluding transaction metric, simply noting those. So, for example, the FAP would simply indicate the MIS(s) that it is not providing data in relation to.

Reliance should be considered innovatively: broader reliance on third parties, when appropriate to do so, would be a welcome extension of the regime.

"Approved entities" and liability for reliance

4.174 Given the "approved entities" approach is inconsistent with FATF standards and no entities have been approved, should we continue to have an "approved entities" approach?

4.175 If so, how should the government approve an entity for third party reliance? What standards should an entity be required to meet to become approved?

4.176 If your business is a reporting entity, would you want to be an approved entity? Why or why not?

4.177 Are there any alternative approaches we should consider to enable liability to be shared during reliance?

BIG's Response

It would make sense if classes of entities such as MIS reporting entities could be relied upon because, the alternative, the licensed managing intermediaries option, is complicated and poorly understood. There is little risk in some classes of reporting entities (as contemplated by section 33(3A)) being replied upon for CDD. As this submission recurringly stresses, CDD is of little value in most cases for the lower risk yet *don't-really-know-their-customers* reporting entities, such as superannuation schemes, and so it would be beneficial if reporting entity #1 (e.g., a Financial Advice Provider) could simply request confirmation that CDD had been completed by "approved" entity #2 without itself having to conduct or retain records relating to CDD which had already been conducted.

If classes of relatively lower risk reporting entities (i.e., low or medium-low sub-sectors of Sector Risk Assessments) were granted "approved entity" status it would increase the efficiency of the regime considerably. There is far too much repetitive activity, especially in

relation to CDD, that serves little purpose in terms of reducing ML/FT yet increases compliance costs. The suggestions here would help reduce that unnecessary cost.

Designated business group reliance

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

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

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

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

BIG's Response

The status quo settings for DBG formation are satisfactory, though they could be extended similarly to the new financial advice regime, which allows for different advice-giving entities to coalesce under a single FAP. Allowing different AML reporting entities to fall under a single DBG where they consider it is appropriate should, by default, be allowed.

Regarding expectations of reporting entities overseas, *providing* the reporting entity is in a jurisdiction of sufficient standing (based on the most recent FATF assessment), there should not be an "imperialist" demand that such entities follow New Zealand requirements in relation to any matter, including CDD. As noted in our response to questions 4.190 and 4.191, below, it is important that there is not a "highest of all jurisdictions" result that increases compliance burdens on New Zealand reporting entities. Similarly, we should not increase the compliance costs of foreign jurisdictions' companies needlessly either.

To illustrate, using this approach for expired passports under the New Zealand Supervisors' requirements: a foreign company member of a New Zealand DBG would be required not to accept any expired passport (by default). However, if a DBG company was Australian, where the AUSTRAC standard is default acceptance up to two years expired, the Australian entity would be required to meet the higher bar set in New Zealand. This is despite Australia being sufficient, jurisdiction-wise, in terms of its latest FATF assessment. The only thing that would be achieved by mandating New Zealand standards on that Australian entity would be increased complexity and compliance cost. There would be no manifest benefit in terms of reducing ML or FT.

Third party reliance

4.182 Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD:
• consider the level of country risk when determining whether a third party in another country can be relied upon;
• take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and
• be satisfied that the third party has record keeping arrangements in place.

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

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

Potential other forms of reliance

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

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

—

Internal policies, procedures, and controls

Compliance programme requirements

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

BIG's Response

The challenge today, which has persisted since the start of the regime, is that there is too much "tick box" compliance with compliance programmes and risk assessments. The minimum requirements are fine insofar as what sections 57 and 58 demand of reporting entities. What's missing is best practice demonstrations to reporting entities of how such requirements are optimally operationalised.

We do not consider, however, that there is need for more prescription. This is because the regime is already prescription heavy. What's really needed is better education and illustration of practical implementations.

The theory, i.e., having policies and procedures in a written form, is necessary, but the more there is (and the more impenetrable it is made due to lots of prescription) carries the risk that those policies and procedures become artefacts which are only brought out when demanded rather than being guides that are regularly used operationally.

Compliance officers

4.188 Should the Act mandate that compliance officers need to be at the senior management level of the business, in line with the FATF standards?

4.189 Should the Act clarify that compliance officers must be natural persons, to avoid legal persons being appointed as compliance officers?

BIG's Response

There should be wider options if the person must be a natural person. One option may be to allow any natural person in the reporting entity/DBG, provided they have an internationally recognised AML/CFT qualification to be the Compliance Officer, regardless of seniority. It is more important that an AMLCO is *competent* than for them to be a *senior manager*. This would also make it easier for smaller reporting entities where it is not always practicable to have an AML/CFT competent specialist at a senior level (e.g., there may only be one or two senior staff).

Group-wide programme requirements

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

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

BIG's Response

Financial group-wide programmes, especially when they span multiple jurisdictions, can be more of a nuisance than a help. It would be helpful if the New Zealand regime specifically demanded that New Zealand reporting entities operate their ML/FT programmes

independently insofar as requiring New Zealand requirements only. This would empower New Zealand reporting entities to categorically disconnect from group demands, which, even if well intentioned, often mean that *both* New Zealand and the reporting entity's Group's (primary country's jurisdiction) ML/FT rules apply. This manifests itself as "whichever is the higher requirement", adds complexity, and consequently increases the compliance burden on New Zealand reporting entities.

Review and audit requirements

4.192 Do we need to clarify expectations regarding reviewing and keeping AML/CFT programmes up to date? If so, how should we clarify what is required?

4.193 Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system?

4.194 What other improvements or changes could we make to the independent audit or review requirements to ensure the obligation is useful for businesses without imposing unnecessary compliance costs?

BIG's Response

The challenge with audits is, especially for reporting entities that have their systems in a good state, is the mandatory, rigid, frequency of re-audits. Fortunately this has been extended recently to every three years, but even that is too much for entities in low or medium-low sectors (per Sector Risk Assessments) with multiple unqualified consecutive audits.

Effectiveness should always be a requirement of an audit. Indeed, other than design, the key assessment purpose of an audit *is* effectiveness?

The deadline for a reporting entity's next audit should be risk-based. The *inherent risk* of the entity's subsector (e.g., casinos clearly should be audited more frequently than KiwiSaver Schemes), as well as the result of the most recent audit, so *residual risk*, should drive the frequency. This would be a much better approach than the uniform three-year requirement that has recently been extended from two years.

A standalone KiwiSaver Scheme, whose most recent audit was unqualified, exemplifies where the requirement could be extended to four, or even more, years by default. Casinos, however, appear appropriate candidates for annual audits, regardless of past performance, given their extremely high inherent risk of ML/FT.

Adding universal, rigid, prescription to reviewing and keeping AML/CFT programmes "up to date" should be avoided. If, however, an explicit "up-to-date" requirement is considered necessary, the inherent risk of sectors and entities, again, should be factored. That is, consistent with our general recommendation regarding a more risk-based regime being appropriate. Put simply, keeping a reporting entity's AML/CFT programme current is more important where the potential for ML/FT is high.

Higher-risk countries

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

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

BIG's Response

Expecting reporting entities to do this analysis is another example of undue compliance cost. A centralised New Zealand "ML/FT country risk list" would make this simple and consistent.

This could also include sanctions flags, making it easy for entities to know which countries are subject to sanctions, something that is not as easy as it should be today.

A Code of Practice is *not* an ideal delivery method, however. They are inevitably interpreted too rigidly. For example, if a KiwiSaver Scheme has one client in Afghanistan due to the member emigrating to return to their family it should not be a big concern per se. However, our members know from dealing with international corporations, for example, that some jurisdictions are very black-and-white when it comes to any connection whatsoever with a sanctioned country.

Imposing countermeasures where called for by the FATF

4.196 Should we issue regulations to impose proportionate and appropriate countermeasures to mitigate the risk of countries on FATF's blacklist?

4.197 If so, what do you think would be appropriate measures to counter the risks these countries pose?

4.198 Is the FATF blacklist an appropriate threshold? If not, what threshold would you prefer?

BIG's Response

Regardless of the rules adopted, it needs to be clear whether they trump other law. For example, the unalienable right to KiwiSaver membership requires clarity. If, for example, there was a requirement to compulsorily exit and pass the exited member's KiwiSaver funds to an independent body (which could then determine whether the funds should be paid out to the member) is a possible scenario. Whatever is done in this space, it should not place the compliance burden on reporting entities to determine what action to take, especially where there is a conflict of laws.

Imposing sanctions on specific individuals or entities

4.199 Should we use section 155 to impose countermeasures against specific individuals and entities where it is necessary to protect New Zealand from specific money laundering threats?

4.200 If so, how can we ensure the power is only used when it is appropriate? What evidence would be required for the Governor General to decide to impose a countermeasure?

4.201 How can we protect the rights of bona fide third parties?

4.202 Should there be a process for affected parties to apply to revoke a countermeasure once made? If so, what could that process look like?

—

Suspicious activity reporting

Improving the quality of reports received

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

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

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

BIG's Response

Instead of asking how the quality of reporting could be improved, it is better to ask how to make it really easy to provide FIU with information. If the process was as easy as typing a short email of what was observed and what looks unusual and then hitting "send", it is likely that the volume of information that FIU receives could exponentially increase and it could request further information on the reports of most interest. The mechanism today is a barrier to the flow of information.

Further better guidance and feedback is needed. Since the commencement of the AML/CFT regime, there have been thousands of SARs lodged. Nevertheless, there is no clear picture of what SARs wasted FIU's time versus those that were immediately escalated and/or led to enforcement action. The lack of visibility in this area is one of the big deficiencies of the regime. It is a "black hole": SARs, like light, go in, yet nothing comes out.

If high quality reporting to FIU is desired, which we hope everyone wants, much more help to reporting entities is required to ensure that those SARs worth reporting are reported and those that aren't don't get reported.

Further, the compliance cost of reporting a SAR is considerable. It takes a long time, usually by Compliance staff, to load SARs into FIU systems. That in itself is a disincentive to reporting entities to report SARs. As noted in the introductory paragraph to this answer, we consider that there should be a "lite" version for lower risk entities to report things that appear a somewhat suspicious but, realistically, are not that likely to be ML/FT.

Another aspect that needs revision is the timeframe for submission of a SAR once suspicion is formed. It is another example of a non-risk-based requirement, being a three-day deadline. In some instanced that may be too slow – e.g., if the suspicion was relating to somebody the entity was aware was emigrating imminently, whereas in most cases the requirement is too extreme – most SARs we expect are not even considered by FIU soon after submission. What would work better is to require instances where the entity has grave concerns that the SAR be escalated directly and with urgency but for the bulk of routine SARs, that a "reasonable" timeframe be specified in which to submit them.

Sharing SARs or SAR information

4.206 Should we expand the circumstances in which SARs or SAR information can be shared? If so, in what circumstances should this information be able to be shared?

BIG's Response

Sharing with supervisors and reporting entity groups would be helpful so as assist other keep a look out for similar activities.

4.207 Should there be specific conditions that need to be fulfilled before this information can be shared? If so, what conditions should be imposed (e.g. application to the FIU)?

—

SAR obligations for MVTS providers

4.208 Should we issue regulations to state that a MVTS provider that controls both the ordering and beneficiary ends of a wire transfer is required to consider both sides of the transfer to determine whether a SAR is required? Why or why not?

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

—

High value dealer obligations

4.210 Should we extend additional AML/CFT obligations to high value dealers? Why or why not? If so, what should their obligations be?

4.211 Should all high value dealers have increased obligations, or only certain types, e.g., dealers in precious metals and stones, motor vehicle dealers?

4.212 Are there any new risks in the high value dealer sector that you are seeing?

—

PART 5: Other issues or topics

Cross-border transportation of cash

When reports should be filed for unaccompanied cash

5.1 Should the AML/CFT Act define the point at which a movement of cash or other instruments becomes an import or export?

5.2 Should the timing of the requirement to complete a BCR be set to the time any Customs trade and/or mail declaration is made, before the PART 5 item leaves New Zealand, for exports, and the time at which the item arrives in New Zealand, for imports?

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

—

Sanctions for falsely declared or undeclared cash

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

—

Powers to search and seize cash to investigate its origin

5.5. Should the Act allow for Customs officers to detain cash even where it is declared appropriately through creating a power, similar to an unexplained wealth order that could be applied where people are attempting to move suspiciously large volumes of cash?

5.6. If so, how could we constrain this power to ensure it does not constitute an unreasonable search and seizure power?

—

Other forms of value movement

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

—

Privacy and protection of information

Requiring mandatory deletion of financial intelligence

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

BIG's Response

As noted in our answer to question 4.77, above, the current expectations around record disposal are aspirational and/or unrealistic in a 21st Century context. Once created, is almost impossible to entirely expunge data since backups and versioning are ubiquitous and inherent features of modern software and SaaS offerings. Requiring mandatory deletion sounds fine in theory, but the reality is it rarely occurs in practice because it is impracticable and/or would be a massive compliance cost if actually enforced.

Requiring mandatory deletion of financial intelligence

5.9 Should we specify in the Act how long agencies can retain information, including financial intelligence held by the FIU?

5.10 If so, what types of information should have retention periods, and what should those periods be?

—

Legally privileged information

5.11 Does the Act appropriately protect the disclosure of legally privileged information? Are there other circumstances where people should be allowed not to disclose information if it is privileged?

5.12 Is the process for testing assertions that a document or piece of information is privileged set out in section 159A appropriate?

—

Harnessing technology to improve regulatory effectiveness

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

BIG's Response

Enabling direct access for reporting entities to official data sources would be a big technological improvement. For example, if a reporting entity could directly request verification against driver licence, passport, and RealMe datasets, that would be welcomed by many.

Challenges and barriers that exist to adopting technology include:

1. *Cost*. The price point for much of the technology available to firms is simply too high. Much of that has to do with the lack of scale in New Zealand (something that could be improved with official data sources access as well as our suggestion regarding a centralised PEP screening Pharmac-like arrangement).
2. *Standalone systems*. These systems while effective in what they do, they do that independently of other back-office systems requiring integration and APIs. All of this is costly and takes resources away from business developments that drive growth versus compliance.
3 *Rigidness of the Act and guidelines*. It's hard to invest in technology when you are uncertain as to your supervisor's views on the technology and its compliance with the Act. It's easy to say reporting entities must do due diligence but that's not very helpful when you are unsure whether the technology being promoted to you is going to be compliant with the Act or find favour with your supervisor.

Enabling the adoption of digital identity

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

BIG's Response

If there is a sufficient "carrot", i.e., have a digital ID and *never have to complete CDD ever again* (other than perhaps proving that a digital ID is in facts yours), that would be a huge gain. The time, energy, and cost for all involved in completing CDD repeatedly cannot be overstated. It is a huge cost to reporting entities and a huge waste of time for New Zealanders. Whatever Digital Identity Trust Framework is adopted needs to ensure seamlessness for customers and reporting entities so as to quickly establish business relationships with minimal "friction".

Establishing a digital identity trust framework is potential great leap forward for New Zealanders. It would be very disappointing if the AML/CFT Act did not work harmoniously with the DITF. Reporting Entities should not be left to make interpretations themselves or have to navigate differing guidelines, for example. This will require the AML/CFT Act to include the provisions necessary that adopting the DITF is seamless and simple for reporting entities and, most crucially, will not put them in a position of conflict with the AML/CFT Act.

Harmonisation with Australian regulation

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

BIG's Response

Provided the New Zealand regulation specifically requires New Zealand entities to only meet New Zealand requirements and overtly not be obliged to meet Australian requirements harmonisation does have some benefits to trans-Tasman reporting entities.

Specifically, there is opportunity to have greater harmonisation also where it would make it easier for New Zealanders. A prime example is acceptance of expired passports. The decision by the New Zealand Supervisors a few years ago was disharmonious. Many reporting entities had defaulted to the AUSTRAC guidance (two years). This was efficient, low risk, and harmonious. As expired passports are not used for travel, only ID validation, as an official government-issued document whether it's expired or not is inconsequential. The part that matters is whether the person still *looks* like their passport photo. For most people, even passports that expired several years ago are fine from that perspective.

The point being: the Australian regime worked better than the more onerous requirements that the NZ Supervisors devised. And that requirement (i.e. no default acceptance of expired passports) aside from be a clear distinction from the Australian AML/CTF regime, added *nothing* to ML/FT prevention. All it did was add compliance cost to reporting entities in having to devise new processes to provide exceptions and made it harder for some New Zealanders to access financial products. Older New Zealanders especially were disadvantaged by this change as they frequently have no preferred current ID documents (as they are less likely to travel overseas and less likely to drive), but often have their expired documents.

Ensuring system resilience

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

The AML/CFT system can best achieve resilience by allowing for more flexible risk-based compliance processes. If this had been fostered initially (for example, on CDD processes), the impact on reporting entities would have been much less. For example, some of our members have continued to onboard customers during the COVID-19 pandemic by putting in place temporary exceptions (for predominantly low risk customers) when customers are unable to fully meet our onboarding requirements

Once COVID restrictions end, we are notionally required to revisit the exceptions to bring the ID documentation collected up to requirements. This would be a significant resource commitment and, importantly, more than an inconvenience for customers, who will be no doubt wondering why many months after we have onboarded them, we are now following up with them for certified documentation. A regime which allowed flexibility, based on risk, would deliver a much better experience for these low-risk clients.

PART 6: Minor Changes

6.1 What are your views regarding the minor changes we have identified? Are there any that you do not support? Why?

6.2 Are there any other minor changes that we should make to the Act or regulations?

The following are responses to a small number of the specific issues and their proposals (solely within the Preventive Measures section of Part 6).

Definitions and terminology

—

Information sharing

—

SARs and PTRs

—

Exemptions

—

Offences and penalties

—

Preventive Measures

Issue: Businesses are required to "have regard" to the factors set out in section 58(2) when conducting a risk assessment. This includes any applicable guidance material produced by AML/CFT supervisors or the Police, such as the National Risk Assessment or the various sectoral risk assessments. However, the language of "have regard to" could allow businesses to consider, but ultimately reject, government advice about national or sectoral risks and therefore fail to implement appropriate controls.
***Proposal*: Amend section 58(2) to ensure that a business' risk assessment reflect government advice about national and sectoral risks.**

BIG's Response

We **do not support** this proposal.

Some higher risk features identified within Sector Risk Assessments may be inapplicable to some reporting entities despite being in a sector/sub-sector. For example, if a reporting entity is "closed to new business" many risks evaporate. Consequently, care should be taken in having language that requires a reporting entity's Risk Assessment to "reflect" a SRA. The current "have regard to" provides appropriate flexibility. If this proposal is progressed, it should have a "carve out": i.e., something like "reflect, except where the entity does not have key characteristics material to the risk associated with its sector" or something to that effect.

Also, if it is a requirement to simply adopt advice, then it is not advice, it is a rule making power. An unfettered unilateral rule making power sitting with the same party that enforces the law is inappropriate and unconstitutional.

Issue: Businesses do not have an explicit obligation to verify any new information obtained through ongoing CDD, except where enhanced CDD is triggered.
***Proposal*: Issue a regulation which explicitly requires businesses to verify any new information obtained through ongoing CDD.**

BIG's Response

We **do not support** this proposal.

This would add unnecessary compliance cost. As we have stated throughout our submission, CDD is of little value in 99%+ of cases where it is gathered. No increased requirements regarding CDD should be introduced unless they are limited to only higher risk entities and/or higher risk sectors.

Issue: There is no requirement that copies of records must be stored in New Zealand, particularly copies of customer identification documents.
***Proposal*: Issue a regulation which requires businesses to retain copies of records in New Zealand to ensure they can be easily accessible when required.**

BIG's Response

We **do not support** this proposal.

It does not reflect that many entities' records are stored in cloud services. Such services are usually not New Zealand-based. Such a requirement as proposed would not reflect the reality of the 2020s, i.e. we are in a global economy. The expectation that records be readily accessible is reasonable, but the mandatory location of New Zealand is not.

Issue: There is a current Ministerial exemption in place that enables members of a DBG (that are reporting entities) to share a compliance officer, subject to certain conditions. The intent is to reduce compliance burden across members of a DBG.
***Proposal*: Amend the Act to allow members of a DBG to share a compliance officer.**

BIG's Response

We **support** this proposal. It is a common-sense change.

Appendix 1

Licensed MIS Managers supporting this submission:

AMP Wealth Management New Zealand Limited

Aspiring Asset Management Limited

Harbour Asset Management Limited

Milford Funds Limited

Mint Asset Management Limited

Nikko Asset Management New Zealand Limited

Norfolk Mortgage Management Limited

Appendix 2

The following sector ratings are taken from the Supervisors' sector risk assessments (noting as the FMA's latest sector risk assessment was released only the same week as this submission was finalised it has not been used).

Financial Markets Authority

https://www.fma.govt.nz/assets/Reports/AMLCFT-Sector-Risk-Assessment-Report-2017.pdf

Page 4

Sector	Sector risk 2017
Derivatives issuers	High
Brokers and custodians	Medium–high
Equity crowd funding platforms	Medium–low
Financial advisers	Medium–low
Managed investment scheme managers	Medium–low
Peer-to-peer lending providers	Medium–low
Discretionary investment management services	Medium–low
Licensed supervisors	Low
Issuers of securities	Low

Reserve Bank of New Zealand

https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/SRA-2017.pdf?la=en

Pages 4 and 5

Sub-sector		Inherent risk of ML/TF
Registered banks – overall inherent risk rating		High
	Retail	High
	Business/Commercial	High
	Wholesale/Institutional	Medium
Non-Bank Deposit Takers – overall inherent risk rating		Medium
	Deposit Taking Finance Companies	Low
	Building Societies	Medium
	Credit Unions	Medium
Life Insurers – overall inherent risk rating		Low

Department of Internal Affairs

https://www.dia.govt.nz/diawebsite.nsf/Files/AML-CFT-December-2019/$file/Financial-Institutions-SRA-2019.pdf (noting DIA has several; this is but one)

Page 6

Sector – Financial Institutions	Inherent risk of ML/ TF 2019	Inherent risk of ML/TF risk 2011	Sector – DNFBPs & Casinos	Inherent risk of ML/TF 2017	Inherent risk of ML/TF 2019
Money remittance	High	High	Trust and company service providers [4]	High	High
Virtual asset service providers	High	n/a[5]	Lawyers	Medium-high	Medium-high
Currency exchange	Medium-high	Medium	Accountants	Medium-high	Medium-high
Payment provider	Medium-high	n/a	Real estate agents	Medium-high	Medium-high
Non-bank non-deposit taking lenders	Medium	Low	High-value dealers	Medium-high	Medium-high
Non-bank credit cards	Medium	Low	Racing Industry Transition Agency	Medium-high	Medium-high
Stored value cards	Medium	n/a	Casinos[6]	Medium-high	Medium-high
Cash transport	Medium	Medium	Conveyancers	Low	Medium
Tax pooling	Low	n/a			
Debt collection	Low	Low			
Factoring	Low	Low			
Financial leasing	Low	Low			
Payroll remittance	Low	Low			
Safe deposit boxes	Low	Medium			