## aml

**From:** [redacted]@kiwiwealth.co.nz>
**Sent:** Friday, 10 December 2021 2:50 pm
**To:** aml
**Subject:** RE: AML consultation submission
**Attachments:** Kiwi Wealth AML CFT Consultation Reponse Dec 2021 FINAL.pdf

Afternoon Nick,

Please find attached Kiwi Wealth's submission on the AML/CFT regime consultation.

If you have any questions, please do reach out to me.

Cheers

[redacted]

[redacted] **| Head of Risk and Compliance**
Kiwi Wealth

Kiwi Wealth. It's wealth. For Kiwi.

[redacted]
W: [redacted]@kiwiwealth.co.nz

Kiwi Wealth includes Kiwi Wealth Limited, Kiwi Wealth Investments Limited Partnership and Kiwi Investment Management Limited

Freepost 210729
PO Box 50617, Porirua 5240, New Zealand

---

**From:** aml <aml@justice.govt.nz>
**Sent:** Monday, 6 December 2021 1:13 pm
**To:** [redacted]@kiwiwealth.co.nz>
**Subject:** RE: AML consultation submission

Kia ora Steve,

Yes, happy to – would an extension until Friday work?

Ngā mihi,

Nick

MINISTRY OF JUSTICE Tāhū o te Ture

[redacted]
Criminal Law | Policy Group
[redacted]

www.justice.govt.nz

*Mon Tues Wed Thur Fri*

**From:** [redacted]@kiwiwealth.co.nz>
**Sent:** Monday, 6 December 2021 12:54 pm
**To:** aml <aml@justice.govt.nz>
**Subject:** AML consultation submission

Morning,

Apologies in advance, are we able to get an extension to be able to give feedback for the AML consultation please?

Cheers

[redacted]

[redacted] **| Head of Risk and Compliance**
Kiwi Wealth

Kiwi Wealth. It's wealth. For Kiwi.

M: [redacted]
W: [redacted]@kiwiwealth.co.nz

Kiwi Wealth includes Kiwi Wealth Limited, Kiwi Wealth Investments Limited Partnership and Kiwi Investment Management Limited

Freepost 210729
PO Box 50617, Porirua 5240, New Zealand

---



---

[redacted]

Kiwi Wealth House

Level 13/20 Ballance Street

Wellington

6011

AML/CFT Consultation Team

Ministry of Justice

SX 10088

Wellington

6140

Email: aml@justice.govt.nz

Dear Sir/Madam,

Please find below Kiwi Wealth's feedback in relation to the current consultation on the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

Kiwi Wealth welcomes the opportunity to provide feedback on the consultation and expresses those views with the intention to continue to comply with the Act and contribute towards the improvements to New Zealand's Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) regime.

The feedback below in Appendix 1 refers to the Review of the AML/CFT Act Consultation Document and the request for information on specific topics, as well as raising areas of concern and/or improvement to the AML/CFT regime that relates specifically to Kiwi Wealth on an exception basis.

If you wish to discuss any of the feedback please contact me directly at [redacted]@kiwiwealth.co.nz or [redacted]

Yours sincerely,

[redacted]

Head of Risk and Compliance (and Anti-Money Laundering and Countering Financing of Terrorism Compliance Officer)

**Appendix 1**

| Ministry of justice question | Kiwi Wealth response |
|---|---|
| How is the Act operating? Is it achieving its purposes? Are there any areas of risk that the Act does not appropriately deal with? | There are a number of issues with a lack of definitions and what a "review" means in relation to ongoing CDD. The concern is that due to a combination of a lack of guidance, and limitation to definitions, there is poor interpretation by reporting entities. We believe that supervisors are under-resourced to be able to effectively manage this issue. This leads to varying standards being used, which leads to some reporting entities not complying and being very easy to onboard with, while others apply more stringent, and often over-comply with CDD requirements. This also leads to some entities spending too little or too much on AML/CFT requirements based on their inherent risk. This leads to customer angst and reporting entities are impacted greatly when remediation is required.<br><br>Kiwi Wealth agrees with the risk-based regime and applies this to its AML/CFT programme. More prescriptive guidance would be useful that could include how to apply a risk-based approach across the different requirements of the Act. A document similar to the Joint Money Laundering Steering Group in the UK would be beneficial (done through consultation of course).<br><br>Other than section 33, the Act does not appropriately deal with reporting entities being able to sell or purchase large customer portfolios. For instance, when one reporting entity sells a part, or all, of a portfolio to another reporting entity as a going concern, the Act sees this as the end of a customer relationship with the seller, but a new relationship with the new reporting entity. However, as a going concern, the purchaser would want to see whether a SAR had been filed or retain ongoing account monitoring alerts and results.<br><br>Address verification, other than for high risk customers, should be removed. Issues with |

| | |
|---|---|
| | address verification causes some of the most contentious concerns for customers and reporting entities with no obvious benefit for police and enforcement.<br><br>A single supervisor model may assist with streamlined interpretation and guidance.<br><br>The Act specifies that reporting entities should file a SAR if we have reasonable ground for suspicion of crimes listed in the Crimes Act. However, domestic based fraud (ie. Doesn't have an international component to it) is not required to be sent to the FIU. The impact of having to do a SAR for all fraud cases would have significant implications for banks and the FIU to process them. However, the true purpose of the Act is not being utilised. It is difficult to know how authorities would deal with fraud cases as there does not appear to be a joined up national response to fraud. This is especially prevalent in the current market and COVID scams (as well as the dozens of other scam types). If there was a coordinated national approach to this then filing a SAR, under certain circumstances, would benefit NZ and contribute to the Acts purpose. |
| What is working and what is not? Are there areas that are particularly challenging or costly to comply with? How could we alleviate some of those costs while also ensuring the effectiveness of the system? | The Code of Practice has recently been updated. However, there needs to be greater collaboration with reporting entities and more detailed information to help reporting entities meet electronic verification requirements. Ideally, reporting entities would benefit from supervisors agreeing to an approved list of providers, as it has done with Real Me. The costs to confirm, test, and ensure compliance with the code from an EV perspective is difficult and costly for most entities.<br><br>The code of practice, and its current standard, closes out future engagement with portions of customers. An example is children or reporting entities with no branch network. Digitally, children are required to have their name verified by two sources. This is unlikely to be achievable as most NZ citizens have a record on births, deaths and marriages, but no other |

| | |
|---|---|
| | electronic database. We understand that the supervisors do not consider IRD data to be reliable to use for these purposes.<br><br>A single government database should be able to be used (call back service similar to DIA confirmation service) that includes all reliable and independent data sources. |
| What could we do to improve the operation of the Act? | The supervisors should have more resources to be able to focus on guidance and wider consultation. Currently consultation appears to be limited to a few entities. |
| Is there anything we need to do to "future proof" the Act and ensure it can respond to the modern and largely digital economy? | The supervisors need to have the appropriate resources to help more entities. See comments above about what is and isn't working in the Act (specifically with regards to children). |
| 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? | The Act should allow information sharing (without the need to have a request received by) with any government agency in the interest of detecting and deterring ML/FT. Currently information sharing is limited. |
| 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? | No, the police actively prevent with the information they receive from SARs and information requests and production orders. |
| 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? | No, although that assumes that this isn't already captured in the financing of terrorism aspect and various acts that a SAR should be filed against. |
| 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? | Kiwi Wealth supports that the purpose should be more general and this will support a future proofed Act. |
| 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? | Yes. The Act is a compliance act and so it would be worthwhile to add Sanctions compliance into the existing regime. |
| 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? | Continue to update the National Risk Assessment. |
| 1.9 What is the right balance between prescriptive regulation compared with the risk-based approach? Does the Act currently | There is not currently enough understanding as to how a risk-based approach can be applied practically. Further prescription of how a risk |

| | |
|---|---|
| achieve that balance, or is more (or less) prescription required? | based regime can be applied should be provided as examples in the various guidelines. |
| 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? | Yes, identification should continue to have a standard. However, we don't believe that the code is future proofed to enable it to be used across increasing use of digital onboarding, especially for those who do not have many electronic records, or are not NZ citizens. |
| 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? | Yes, exemptions are still required. However, even when a low risk entity (such as a charity) is captured they should continue to be captured but with reduced requirements (rather than wholly exempted). True low risk should be considered on an inherent risk basis, not considering the controls (residual). |
| 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? | MOJ should be the decision maker as they provide an impartial, non-bias view, and have a global view of FATF requirements. |
| 1.16 Are the factors set out in section 157(3) appropriate? | Yes. However, there should be a weighting system applied so that one factor is more important than another. |
| 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? | Yes. Proven low risk should be based on a reporting entities inherent risks. |
| 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? | There should be a simplified process. |
| 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? | As an exempt entity is essentially not a reporting entity, no supervisor therefore ensures that the exempted entity is complying with any condition/s of the exemption. This is a gap in the regime. |
| 1.21 Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done? | Many reporting entities do not employ AML expertise. This is called out in the RBNZ SRA which indicates a lack of AML knowledge as a vulnerability. A risk based approach should be used, but most entities do not know how, or when to apply it. Therefore, more prescription is required to meet the goal of the legislation. |
| 1.22 How could the regime better protect the need for people to access banking services to properly participate in society? | See comments about the code of practice and electronic verification in response to how the Act is operating. |

| | |
|---|---|
| 1.23 Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them? | Concerns with misinterpretation has led to many different approaches to customer onboarding which has led to market advantages/disadvantages. This causes issues for customers and competition issues between reporting entities, often from different industries that sell similar products. Guidance and enforcement are key preventative measures. |
| 1.24 Can the Act do more to enable private sector collaboration and coordination, and if so, what? | Yes, active consultation and engagement with the wider AML community with guidance documents. will allow reporting entities to properly input into the regime with specific market information needed. Alternatively, forming more industry bodies and consulting with more of them will help manage consultation better. |
| 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? | There appears to be issues with the FIU being able to share intelligence with the wider AML community for fear that NZ Police information will get into the wrong hands (as it will be shared widely) and weaken the NZ Police's ability to protect and investigate organised criminal groups. This prevents reporting entities (other than those that are part of the limited group working with FIU) looking to file SARs on actual ongoing crime. |
| 1.26 Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime? | Yes. As above. |
| 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? | The National Risk Assessment can hold this information. The Act could also list how it measures success. This includes meeting information sharing targets, SAR numbers, enforcement and information from supervisors that can monitor improvements in compliance with the Act (as was required for FATF). |
| 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? | Yes. The Act should not limit police, as long as police do this under the right provisions and scrutiny from other independent authorities. |
| 1.29 If the FIU had this power, under what circumstances should it be able to be used? | Court ordered (in the same way that production orders are obtained). |

| | |
|---|---|
| Should there be any constraints on using the power? | |
| 1.30 Should the FIU be able to request information from businesses on an ongoing basis? Why or why not? | Yes. As long as the information was understood and not simply a tick the box exercise and forms part of record keeping requirements. |
| 1.31 If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected? | See above. |
| 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? | Yes. The power would have to be managed and scrutinised by an independent body such as a court. However, the speed to being able to execute this would be a concern that may not make the ability effective. |
| 1.33 How can we avoid potentially tipping off suspected criminals when the power is used? | This would be very difficult. The current regime allows reporting entities the ability to ask for SOF/SOW without tipping off. The key interpretation with regards to tipping off is that a SAR has been filed. Reporting entities would need a reason to not reach out to a customer and it would not be a true breach of the Act unless the existence of a SAR was communicated. |
| 1.34 Should supervision of implementation of TFS fall within the scope of the AML/CFT regime? Why or why not? | Yes. The regime is already set up to add some further detail in. |
| 1.35 Which agency or agencies should be empowered to supervise, monitor, and enforce compliance with obligations to implement TFS? Why? | The three current AML/CFT supervisors could manage this. However, noting a single supervisor would more effectively manage the requirements and communication to reporting entities. |
| 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? | This should be an operational decision making piece which should include MOJ and public consultation. The AML/CFT National Coordination Committee could take the decision making role. |
| 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? | Yes. |
| 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? | The regime would benefit from a risk assessment code of practice. Possibly having 2-3 options on how to do it based on business size. |

| | |
|---|---|
| | The current code of practice isn't detailed enough for electronic verification. The code could be updated more often, and not single out Real Me. It could include approved third-party entities (such as Cloudcheck, Origin ID or APLYID). Having an approved list of entities would have significant cost savings as reporting entities are currently having to consult with both the vendor and supervisor at length. |
| 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? | Yes. However, other than replicating the same concepts to all overseas documentation and electronic sources, there is limited or no options available to be as equally effective for ID in NZ. |
| 1.42 What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool? | They should form a complete and full part of the code of practice and provide significant information to comply. |
| 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? | Yes. Currently the annual report framework is written in legislation and therefore does not allow for supervisors to change the information. However, changes to the annual report should not be often and allow significant lead in time for changes (as well as consultation). |
| 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? | Yes. A risk-based regime is appropriate. However, there is limited industry knowledge on how to apply it either properly or correctly. A Joint Money Laundering Steering Group would be appropriate. |
| 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? | NCC should coordinate. |
| 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? | Yes. This would support the purposes of the Act and allow greater information sharing (noted in other areas of this response). |
| 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? | Yes. This would support the purposes of the Act and allow greater information sharing (noted in other areas of this response). |
| 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 | No, we would not be concerned in filing SARs. The access to mass data would need to be managed at a government level. In many cases, the information is simply spread over |

| | |
|---|---|
| the likelihood of businesses being willing to file SARs? | government. Bringing it together in a cohesive way would benefit wider Government goals. |
| 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? | Yes. This is particularly relevant for DIA and FMA as they supervise entities that do not require a licence to operate. This would allow those supervisors to better use their resources. |
| 1.53 If such a regime was established, what is the best way for it to navigate existing registration and licensing requirements? | Use of the existing licencing regime in NZ. This would be co-ordinated through the supervisors. The supervisors could issue a compliance notebook or similar on the requirements of the Act and how to comply. |
| 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? | No. |
| 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? | Potentially. However, how an entity would be rated would need to be worked through. |
| 1.58 If such a regime was established, what is the best way for it to navigate existing licensing requirements? | Create legislation like the non-bank deposit takers legislation and set up a regulator and supervisor. |
| 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? | The current regime has identified issues with de-risking. Legitimising businesses through licencing (which could include a need to have an AML RA and Programme) will reduce the impacts on businesses maintaining a bank account and reduce the risk of ML/FT. |
| 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"? | Guidance should be able to cover this off. |
| 2.3 Should "ordinary" be removed, and if so, how could we provide some regulatory relief for businesses which provide activities infrequently? Are there unintended consequences that may result? | Businesses that conduct activities, even if infrequently, should be captured by the requirements of the Act. There is an argument that if infrequent activities aren't captured, then a ML/FT risk will emerge in that this loophole could easily be targeted by organized crime groups and/or lone actors. |
| 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? | Yes. DNFBP's have been identified in many cases to be an inherent high risk to ML/FT. Reduced measures have been given to many in the Act, due in part due to the cost of compliance. However, these businesses are |

| | |
|---|---|
| | inherently high risk to ML/FT and should be required to be captured by the full requirements of the Act to ensure the purpose of the Act is maintained. We note that some DNFPB's are the first gateway of moving illicit funds into the financial system through cash and sales and purchase of high value goods. |
| 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? | Yes. The captured activity should drive the requirement to be subject to AML/CFT requirements, not the business type conducting the activity. |
| 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? | Yes. See response to 2.4. |
| 2.18 Should we lower the applicable threshold for high value dealers to enable better intelligence about cash transactions? Why or why not? | Yes. See response to 2.4. |
| 2.29 If so, should non-life insurance companies have full obligations, or should they be tailored to the specific risks we have identified? | Yes. In a limited way which reduces compliance requirements while mitigating the risks posed. |
| 2.35 Should preparing accounts and tax statements attract AML/CFT obligations? Why or why not? | Potentially. As long as this relates to specific accounting businesses (not Kiwi Wealth who produce tax statements for customers). If there is an ability to identify predicate crimes such as tax evasion or evidence of trade-based ML. Financial auditors may be in a better position to identify these predicate crimes, or potentially internal (employee) fraud. |
| 2.36 If so, what would be the appropriate obligations for businesses which provide these services? | A limited, reduced compliance requirements regime for accounting business, based on specific SAR obligations may suffice. |
| 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? | Class exemptions should be reviewed periodically to ensure they are still fit for purpose and have evidence of low/no risk (inherent). |
| 2.56 Should the AML/CFT Act define its territorial scope? | Yes. It is important for many reporting entities and a complete list of definitions in the Act is required to clear up many misinterpretations by reporting entities. |
| 3.1 Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it? | No. |

| | |
|---|---|
| 3.2 If it were to change, what supervisory model do you think would be more effective in a New Zealand context? | A single supervisor model would benefit reporting entities. With the right mix of industry knowledge through recruiting experts would negate the perceived issues with moving to a single model. Reporting entities require clear and consistent messaging and interpretations. The three current supervisors do try and ensure consistency but it can be difficult. |
| 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? | Not always. We believe a single supervisor would help. |
| 3.5 Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why? | The publication of codes of practice would be useful. These should be managed through NCC rather than Ministers. |
| 3.9 Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient? | Yes. |
| 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? | Yes. A code of practice could be published to ensure a prescriptive and thorough audit is completed. This may negate the need to have approved auditor lists as long as the audit (which the reporting entity would need to follow or opt out of a code) requirements are followed. |
| 3.12 Who would be responsible for enforcing the standards of auditors? | Reporting entities (based on the response to 3.11). |
| 3.18 Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for? | Yes. We use them to complete CDD. |
| 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? | A guidance document, or code of practice, would benefit reporting entities so they can understand what they can use an agent for (for eg. CDD, SARs, ongoing CDD) and how to manage the ongoing relationship. |
| 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? | Yes. As a general rule, and internationally cases of note. Reporting entities often only take action once strict enforcement is met. Enforcement drives dissuasive movement within reporting entities and engages senior management in AML/CFT requirements. A proactive approach to AML/CFT rather than reactive (and possibly a business decision being taken with the thought that supervisors are |

| | |
|---|---|
| | light touch) should be established in the regime. This also meets FATF standards. |
| 3.27 Should compliance officers also be subject to sanctions or provided protection from sanctions | Yes. There should be clear protections for compliance officers as long as their actions are not negligent. |
| 4.1 What challenges do you have with complying with your CDD obligations? How could these challenges be resolved? | See commentary on digital electronic verification and address verification in the response to whether the Act operating appropriately. |
| 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? | Yes, it is difficult toonboard minors. This is especially important as the Government wishes for all New Zealanders to save for their retirement. |
| 4.5 Do you anticipate that there would be any benefits or additional challenges from a more prescriptive approach being taken? | No. |
| 4.10 For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear? | No, it is not clear asthere is no definition. |
| 4.11 Should CDD be required in all instances where suspicions arise? | Yes. Noting that this should only be a requirement if FIU agree that this requirement is necessary. |
| 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? | If the ID is not up to standard of the code. Plus EDD (SOF/SOW) on suspicion as already required. |
| 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? | Issue guidance (via GoAML rather than published guidance on websites). |
| 4.18 Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed? | No. Address verification should be risk based. Only high-risk customers. |
| 4.20 Is the information that businesses should obtain and verify about their customers still appropriate? | No. See response to 4.18. |
| 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? | Yes. The source of funds is usually associated with a specific concern and suspicious transactions, rather than the overarching source of wealth which would be more applicable to initial onboarding and knowledge for transaction monitoring. |
| 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? | Ideally, Source of Funds should be obtained when there is a suspicion. This may lead to a transaction being deemed non-suspicious after this is obtained. |

| | |
|---|---|
| 4.27 Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds? | Potentially. The view of FIU with regards to records of SOF/SOW should be required to evidence the need for this and meet the Acts purpose. |
| 4.30 Have you encountered issues with the definition of a beneficial owner? If so, what about the definition was unclear or problematic? | No |
| 4.31 How can we improve the definition in the Act as well as in guidance to address those challenges? | Update beneficial ownership guidance with the enhancements needed to meet the FATF ME recommendations and the ultimate beneficial ownership requirements (as seen in the EU directives). |
| 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? | Yes. Align with EU directives. |
| 4.33 To extent are you focusing beneficial ownership checks on the 'ultimate' beneficial owner, even though it is not strictly required? | Yes. However, consistency of application is required across all industries to ensure the same approach is taken. |
| 4.34 Would there be any additional costs resulting from prescribing that businesses should focus on the 'ultimate' beneficial owner? | Potentially. Administrative and process changes as well as educating employees and customers. |
| 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? | Yes. POWBATIC is poorly understood and applied in NZ. Aligning to an international standard is a better approach. |
| 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? | Reliable and independent documentation (not verbal from the customer) and use of companies office information. |
| 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? | Yes. All guidance is welcomed. |
| 4.41 Would there be an impact on your compliance costs by mandating this process? If so, what would be the impact? | Potentially. Administrative and process changes as well as educating employees and customers. |
| 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 | Yes, although the current guidance mostly covers these requirements. |

| | |
|---|---|
| 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? | Potentially. Administrative and process changes as well as educating employees and customers. |
| 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? | No. Address verification should be removed unless in high risk situations. Noting comments on EV previously in the whether the Act is operating appropriately. |
| 4.45 Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved? | Yes. Remove the requirement to do a second name check for electronic verification as long as the first source is a government source (any government source). The linking mechanism should also be given greater weight in conjunction with the name and date of birth verification or an allowance to use different combinations. |
| 4.46 Is the approach in IVCOP clear and appropriate? If not, why? | Yes. Noted in previous comments in the whether the Act is operating appropriately. |
| 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? | Yes. |
| 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? | Yes. Government sources should be reliable to be able to be used. Reporting entities would benefit from access to the underlying photo evidence of customers so to reduce the impact on customer onboarding and customer irritation. There needs to be a joined up approach at a government level to make this happen. |
| 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? | Yes. Noted in previous comments in the whether the Act is operating appropriately. |
| 4.50 What challenges have you faced with verification of address information? What have been the impacts of those challenges? | Customer addresses, and the complexities with electronic address matches and potential for fraudulent paper copies, means customers are often failing onboarding. The percentage is >10% at onboarding electronically and has an impact to customers. It is not clearly evidenced why this requirement continues to be required. |
| 4.51 In your view, when should address information be verified, and should that verification occur? | High risk situations only. |

| | |
|---|---|
| 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? | Remove the requirement except in high risk circumstances. |
| 4.53 Do you currently take any of the steps identified by the FATF standards to manage high-risk customers, transactions or activities? If so, what steps do you take and why? | Yes. EDD, enhanced OCDD also. |
| 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? | Yes. All guidance welcomed. |
| 4.55 Should any of the additional measures be mandatory? If so, how should they be mandated, and in what circumstances? | This should be explored through consultation. |
| 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? | Code of Practice would be welcomed. |
| 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? | No. As long as FIU agree with the current approach and evidence of crime and NZ family Trusts continues. NZ has many Trusts. However, FIU evidence suggests that NZ Trusts (incl. family Trusts) are often involved in and how illicit assets. Simply because NZ has lots of Trusts which do mask ownership, doesn't negate the need to manage the risk appropriately. If we remove the need to conduct appropriate CDD, and SOF/SOW, then Family Trusts will become even more vulnerable to ML. Especially with the impact of a UBO requirement. So the regime requires more scrutiny of UBO, not less. The risks of a Family Trust reduce once CDD has been completed. And the management of Family Trusts can and should, and is at KW, managed differently to higher risk Trusts and foreign Trusts. |
| 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? | More guidance on what defines a higher risk trust and definition of foreign Trusts. |
| 4.61 Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making? | No. Definition is required as to what a "Review" entails. This is not explicit in the Act and there is currently no guidance. The review should define whether transaction monitoring is |

| | |
|---|---|
| | required at review, whether ID standards should be uplifted to the current standard, and whether up to date SOF/SOW is required (which it should not unless another risk emerges). |
| 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? | Yes. |
| 4.63 Should we issue regulations to require businesses to consider these factors when conducting ongoing CDD and account monitoring? Why? | Yes. |
| 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? | Potentially. That would depend on whether the new regulations required Kiwi Wealth to do more than we currently do. However, we would expect consultation on any new regulations which would include the cost implications of new regulations. . |
| 4.65 Should we mandate any other requirements for ongoing CDD, e.g. frequently it needs to be conducted? | No. The current Risk based approach is appropriate and should be included in any new guidance/code. |
| 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? | Issue guidance. For instance, customers that have been ID to the standard pre Act (Eg. A copy of a DL only is recorded, or a DL number is stored) could be handled in a way that they are ID again to the proper standard on an opportunity basis. |
| 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? | All guidance is welcome. If it is written into the Act, then all entities must comply. |
| 4.76 Do you have any challenges with complying with your record keeping obligations? How could we address those challenges? | No. |
| 4.79 Do you have any challenges with complying with the obligations regarding politically exposed persons? How could we address those challenges? | There are challenges and different interpretations of what a domestic PEP is. Challenges with whether the PEP is overseas, but the spouse or family member is in NZ, so it can be confusing. Bringing domestic PEPs into the Act will remove confusion. |
| 4.81 How do you currently treat customers who are domestic PEPs or PEPs from international organisations? | Domestic PEPs are not considered PEPs by our programme. However, noting response to 4.79. |
| 4.82 Should the definition of 'politically exposed persons' be expanded to include | Yes. Remove the overseas component in the definition. Issue guidance and advise ministers |

| | |
|---|---|
| domestic PEPs and/or PEPs from international organisations? If so, what should the definitions be? | that they will be receiving lots of requests for SOF/SOW in the near future. Educate ministers. |
| 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? | No. |
| 4.84 What would be the cost implications of such a measure for your business or sector? | More high risk customers = more resources required. |
| 4.85 How do you currently treat customers who were once PEPs? | If there are no other risks, such as high risk country, they will be treated as a low risk customer. |
| 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? | Yes. That should be the case anyway. However, the Act would have to mandate that certain positions or risk factors should be treated as such. Currently, occupation is not a mandated requirement to collect at onboarding or OCDD. |
| 4.87 Would a risk-based approach to former PEPs impact compliance costs compared to the current prescriptive approach? | No. |
| 4.88 What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP? | Pay a third party vendor to do the screening. We then triage the alerts and raise escalations to management for approval/decline of relationship. |
| 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? | Reasonable steps is not defined, so it makes it confusing for entities and there is often misinterpretation. |
| 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? | Yes. |
| 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? | No. This would significantly impact the customer onboarding process and given the chance of a customer being a PEP is highly unlikely, this would not appropriately manage the risk. A "day 2" process is appropriate. |
| 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 | Potentially. As long as NZ is still considered in future to be a low risk country to bribery and corruption with officials. The PEP regime may benefit from PEPs being split into low/high risk buckets dependent on the risk of the country they are in to bribery and corruption. Guidance |

| | |
|---|---|
| beneficial owner is a domestic or international organisation PEP? | would need to capture country risk ratings (rather than allowing a free for all) and it would need to be mandated to follow. |
| 4.94 What would the cost implications of including domestic PEPs and PEPs from international organisations be for your business or sector? | Initially, based on current requirements, our customer base would need to be screened to include domestic PEPs and then complete the customer follow up. |
| 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? | No. |
| 4.97 What steps do you currently take to mitigate the risks of customers who are PEPs? | EDD and senior manager approval along with periodic reviews. |
| 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? | Yes. |
| 4.99 What would be the cost implications of requiring businesses to take further steps to mitigate the risks of customers who are PEPs? | See response to 4.94. |
| 4.107 How can we support and enable businesses to identify associates and persons acting on behalf of designated persons or entities? | See response to 4.106. |
| 4.108 Do you currently screen for customers and transactions involving designated persons and entities? If so, what is the process that you follow? | Same as PEPs. They are searched for from a PEP and sanctions perspective. |
| 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? | No. Noting that sanctions risk could (and should be used) be used to identified customers and beneficial owners that may represent higher risk to ML/FT. |
| 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? | A lead in time would be required and access to the supervisor to ask questions. Guidance or a code of practice would be appropriate. |
| 4.158 Should we issue regulations or a Code of Practice to provide more clarity about the sorts of transactions that require a PTR? | Yes. As well as alignment from the supervisors on the interpretation. |
| 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? | If the FIU can evidence the need for lower transaction values then this should be implemented. |

| | |
|---|---|
| 4.171 Do you use any of the reliance provisions in the AML/CFT Act? If so, which provisions do you use? | Yes. Kiwi Wealth is part of a DBG (s32) and also used s33 when completing the sale of a portfolio to another reporting entity. |
| 4.172 Are there any barriers to you using reliance to the extent you would like to? | Yes. In a DBG relationship, Kiwi Wealth is required to conduct full CDD to the standards of the Act (the code) when we onboard a customer that was onboarded with another DBG member but the ID they hold is now expired. Kiwi Wealth believes that we should be able to onboard and rely on ID taken by another DBG member as long as the ID that member took met the code at the time of onboarding. We do not believe the requirement gives further comfort that we are dealing with a real customer. It is costly and impacts customers. |
| 4.173 Are there any changes that could be made to the reliance provisions that would mean you used them more? If so, what? | In a DBG relationship, one reporting entity should be able to fully rely on verification conducted by another DBG member that has been conducted to the standards of the code (at the time of onboarding) and therefore rely on the CDD taken at that time. |
| 4.182 Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD:<br>• consider the level of country risk when determining whether a third party in another country can be relied upon;<br>• take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and<br>• be satisfied that the third party has record keeping arrangements in place. | Yes. This should actually be covered by the reporting entity anyway and so ensuring reporting entities do this to onboard third parties is prudent. |
| 4.183 Would doing so have an impact on compliance costs for your business? If so, what is the nature of that impact? | No. |
| 4.184 Are there any other issues or improvements that we can make to third party reliance provisions? | It is not clear whether obligations other than CDD can be relied on. For instance, whether a third party/vendor (possibly not a reporting entity) can file SARs. |
| 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? | Ensuring reporting entities properly risk rate all customers, and do not outsource or don't risk rate customers at all through those third parties. |

| | |
|---|---|
| 4.189 Should the Act clarify that compliance officers must be natural persons, to avoid legal persons being appointed as compliance officers? | Yes. |
| 4.193 Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system? | Yes. |
| 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? | Lifting the standards of audits to a new minimum standard (as noted in a previous response with regard to a code of practice) would benefit the regime and individual reporting entities. An audit standard, that included information on how to assess material breaches (which are currently dealt with by individual auditors to differing standards), could also help supervisors rely on audits as an effective monitoring tool. |
| 4.197 If so, what do you think would be appropriate measures to counter the risks these countries pose? | An Enhanced CDD framework is an appropriate measure to manage country risk. Parameter led transaction monitoring rules (which is currently in place for many if not all large reporting entities with wire transfer functionality) are also required to manage all country risk appropriately. |
| 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? | Yes. |
| 4.203 How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting? | The system is complicated to use and takes too long to files a SAR. Further guidance is required to ensure quality SARs are submitted and reporting entities can identify reasonable grounds for suspicion of predicate offenses. |
| 4.204 What barriers might you have to providing high quality reporting to the FIU? | GoAML is too complex and requires too much information. Reporting entities focus on filling out the fields in GoAML rather than focusing on the reason for suspicion. |
| 4.205 Should the threshold for reporting be amended to not capture low level offending? | No. This seems to be counter-productive with the purpose of the Act. |
| 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? | Yes. Auditors are currently missing from the Act's list of authorised persons. |
| 5.8 Does the AML/CFT Act properly balance its purposes with the need to protect people's | Yes. |

| | |
|---|---|
| information and other privacy concerns? If not, how could we better protect people's privacy? | |
| 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? | Approved lists of vendors other than RealMe would improve the regime for reporting entities. |
| 5.15 Should we achieve greater harmonisation with Australia's regulation? If so, why and how? | Not necessarily. Requirements are mostly the same (as they should be) but NZ needs to apply laws that are appropriate for NZ. |
| 5.16 How can we ensure the AML/CFT system is resilient to long- and short-term challenges? | The key is that a level playing field is required for all reporting entities to deliver very similar requirements for all customers. This can be achieved through effective guidance, more code of practices, and aligned supervisor feedback and interpretations. The regime requires a joined up approach to electronic sources to ensure customers can easily interact with reporting entities. An approach should be considered that allows customers to move from one reporting entity to another in a way that allows more freedom of choice for customers while still enabling compliance with obligations. |
| ***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.<br>***Proposal*: Amend section 58(2) to ensure that a business' risk assessment reflect government advice about national and sectoral risks.** | Agree with the change. |
| ***Issue***: Businesses do not have an explicit obligation to verify any new information obtained through ongoing CDD, except where enhanced CDD is triggered.<br>***Proposal*: Issue a regulation which explicitly requires businesses to verify any new information obtained through ongoing CDD.** | If this is in relation to name changes, then yes. However, if this is in relation to customers address changes, then no. |
| ***Issue***: There is no requirement that copies of records must be stored in New Zealand, | Given that most businesses are moving their information to cloud based services and |

| | |
|---|---|
| particularly copies of customer identification documents.<br>***Proposal*: Issue a regulation which requires businesses to retain copies of records in New Zealand to ensure they can be easily accessible when required.** | applications any such requirement is unlikely to be feasible. It should allow data to be held outside of New Zealand (eg. In data centres located outside of New Zealand) that the entity accesses through the internet. |
| ***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.<br>***Proposal*: Amend the Act to allow members of a DBG to share a compliance officer.** | Agree with the change. |