NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Ministry of Justice

on the

Review of the AML/CFT Act Consultation Document

17 December 2021

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

About NZBA

1. The New Zealand Bankers' Association (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following seventeen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

3. NZBA welcomes the opportunity to provide feedback to the Ministry of Justice (**MoJ**) on the Review of the AML/CFT Act Consultation Document (**Consultation Document**). NZBA commends the work that has gone into developing the Consultation Document.

Contact details

4. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Brittany Reddington
Associate Director, Policy & Legal Counsel
brittany.reddington@nzba.org.nz

Summary

NZBA looks forward to working with MoJ on this statutory review of the AML/CFT Act (**Act**). Industry engagement will be crucial in ensuring any amendments to the Act are proportionate and fit for purpose and the regime operates as effectively as possible, while not being unnecessarily burdensome on reporting entities. The Consultation Document is a great first step in engaging industry on the review.

Our detailed comments are set out in the table below. We note that we have only answered certain questions. Our key thoughts include:

- **Removal of address verification:** we strongly recommend removing the requirement to verify address information. While address collection can be useful in contributing to the assessment of jurisdictional risk and the prevention of fraud, the current obligation to verify such information is not fit for purpose (noting that residential address can and does change on short or no notice) and can have a disproportionate impact on customers. The impacted customers are often those in vulnerable circumstances, for example, those in transient housing situations or recently released prisoners. We recommend that the obligation to obtain address verification be removed from the CDD section of the Act in all circumstances (including high-risk customers). The Act could retain a requirement for reporting entities to collect this information where available, but not have to verify it.

- **A new 'prevention' purpose may cause difficulties**: we fully support preventing money laundering and financing terrorism, but are concerned that a prevention purpose may unnecessarily cause complexities and be difficult to operationalise. Additionally, there is in our view a risk that a prevention purpose may undermine the suspicious activity reporting regime. We also query how the success of such a purpose would be measured. Please refer to our detailed comments in response to question 1.2.

- **Support for risk-based approach to regulation and supervision:** NZBA supports a risk-based approach to regulation and supervision rather than a prescriptive approach. There are some instances where prescription is appropriate (noted in our answers below), but generally, in our view the regime will operate best if it is focused on risk mitigation rather than being a 'box-ticking' exercise.

- **Industry consultation**: we strongly recommend that early consultation and collaboration with our members is required when developing or changing Codes of Practice and guidance. This is important to help ensure that: any proposals are operationally achievable, will achieve the desired outcomes and will not create any unintended consequences for reporting entities or customers.

NEW ZEALAND BANKERS ASSOCIATION

#	Question	Response
	(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?	NZBA considers that the purposes of the Act are still appropriate for New Zealand's AML/CFT regime.
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?	We understand the desire to move towards a prevention model, and support preventing financial crime, but we have concerns about how this purpose may be operationalised and how achieving this purpose will be measured. Including prevention as a purpose potentially imposes a greater burden onto reporting entities, particularly banks. Our concerns include: • *Safety of staff:* under a prevention model, bank staff may be required to decline transactions. Particularly in small communities, this may lead to awkward conversations or intimidation, with staff feeling threatened. • *Tipping off provisions*: we query how staff would be able to decline a transaction without tipping off the customer about their concerns or suspicions. It is unclear what requirement takes precedence, their obligation to prevent money laundering, or their obligation not to "tip off". • *Staff and bank protections*: would the Act contain any protections for staff if they don't feel comfortable declining a transaction safely, and the customer/third party is ultimately involved in a crime? • *Definition of "suspicion" and thresholds for declining*: the Act would need to contain a very clear definition of what a "suspicion" is, and what the thresholds are for declining a transaction. • *Potential for missed reporting*: if the Financial Intelligence Unit (**FIU**) were to provide clear guidance and thresholds for when transactions must be declined, staff could potentially stop reporting all other transactions that might actually be suspicious and provide valuable intelligence. • *Transactions outside the branch network*: it would likely be easier to decline transactions outside the branch network (e.g. international payments), but there would still need to be clear parameters/thresholds in place.

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

#	Question	Response
		• *Difficulties in 'real time' monitoring*: we note that preventative transaction monitoring would likely be difficult to implement and would result in high compliance costs. It could disrupt well-established banking practices, and negatively impact the majority of customers undertaking transactions for lawful purposes. In our view, there is also a risk that introducing a prevention purpose will threaten the 'suspicious' activity regime – reporting entities may have to move away from suspicion to fact, based on reasons or thresholds set out in the Act. It is unclear whether reporting entities would continue to report all transactions staff consider suspicious, even if they do not meet the legislative definition. We also query what protections reporting entities would be afforded if they decline a transaction on the basis set out in the Act, but the transaction is ultimately legitimate. Aside from legal protections, there is a reputational risk if a customer goes to media or the banking ombudsmen. Additionally, we query how the supervisors/FIU would measure success if this were introduced as a purpose.
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?	In light of the concerns outlined above, our view is that a preventative purpose would work best if primarily directed at enhancing tools for law enforcement, rather than revising obligations for reporting entities (for example, the proposed asset freezing power).
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?	NZBA supports the introduction of a purpose of countering the financing of proliferation of weapons of mass destruction.
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?	In our view it does not make sense to specify particular regions or countries – we recommend the purpose be linked to a sanctions regime which will likely be updated in line with suspected activity in this space (linked to our answer below to question 1.6).
1.6	Should the Act support the implementation of terrorism and proliferation financing targeted financial sanctions, required under the Terrorism Suppression	Yes. In our view, implementing sanctions goes hand-in-hand with countering financing terrorism. Banks operating at a global scale are already required to have sanctions

#	Question	Response
	Act 2002 and United Nations Act 1946? Why or why not?	programmes in place, but we note that this implementation may create significant work for smaller reporting entities. We also query who would supervise this regime, as we note there are limited organisations in New Zealand with experience in this area. We think having one supervisor overseeing this regime is important to ensure consistency.
(1) Institutional arrangements and stewardship – risk-based approach to regulation		
1.7	What could be improved about New Zealand's framework for sharing information to manage risks?	*Increased government feedback* In our view there would be benefits in an enhanced feedback loop from Government agencies (particularly the FIU) to reporting entities. The National Risk Assessments (**NRA**) are helpful documents but are relatively static. The monthly Suspicious Activity Reports (**SAR**) are helpful, but we consider there would be great benefit in receiving regular, direct and targeted feedback and intelligence from the FIU on activity they are seeing and targeting. This would allow banks to develop and enhance their own monitoring tools to assist with identifying this activity. We would also welcome more regular feedback from the RBNZ regarding best practice. For example, reports on what they are seeing in their on-site inspections, what comprises good or bad behaviour, what are their areas of focus and what do they want banks to focus on. *There must be a clear lawful basis for the disclosure of customer information* If it is intended for there to be appropriate sharing and disclosure of customer information, this must be enabled on clear legislative basis.
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?	We view section 58 as still appropriate and do not see a need for change at this stage.
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?	We support retaining the risk-based approach, but think that the Act currently skews more towards prescriptive regulation. We see benefit in moving to a more risk-based regime. Currently, our members' experience is that reporting entities are reviewed against the Act and regulations rather than the outcomes they achieve.

#	Question	Response
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?	In our view there are opportunities to ensure that sections within the Act which carry prescriptive requirements are warranted based on the risk of money laundering or terrorist financing. Otherwise, the requirements should be contextualised by use of 'as warranted by the risk of money laundering/terrorist financing', putting the onus on the reporting entity to assess the risk involved and act accordingly. Supervisors can then engage with an entity on whether or not the risks have been appropriately considered and assessed, and whether or not the actions are adequate. Prescriptive requirements under the Act should be reserved for instances where a risk-based approach is not appropriate or where all reporting entities should have the same position on the risk involved. For example, 'trusts' can carry varying degrees of risk depending on their structure, set-up, and complexity. Having enhanced customer due diligence (**ECDD**) apply in all instances is not risk-based; it carries an administrative burden disproportionate to the risk involved in certain circumstances and doesn't allow reporting entities to apply the customer due diligence measures as warranted by the risk of money laundering or terrorist financing. We would welcome guidance to provide further clarity, particularly in the areas of ECDD and Ongoing Customer Due Diligence (**OCDD**), Beneficial Ownership and Prescribed Transaction Reporting (**PTR**). We also think that reporting entities could benefit from greater transparency and alignment on regulatory supervision and enforcement across the industry among the RBNZ, FMA, DIA and FIU. In our view the Act currently has a "one size fits all" approach in a lot of respects, which may not work well for smaller reporting entities.
1.11	Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?	
1.12	Does the Act appropriately reflect the size and capacity of the businesses within the AML/CFT regime? Why or why not?	
1.13	Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to and the size of the business? If so, what?	NZBA recommends MoJ engage with smaller reporting entities on this question.
1.14	Are exemptions still required for the regime to operate effectively? If not, how can we ensure	Banks are unlikely to use the exemptions process. However, we note that:

#	Question	Response
	AML/CFT obligations are appropriate for low-risk businesses or activities?	• In our view, an exemption should only be given once low, inherent money laundering risk is proven. Otherwise, the purpose and effectiveness of the regime may be undermined. • We support an operational decision maker such as the Secretary of Justice, to expedite the process. • The process for applying for an exemption should be clear and prescribed either in regulations or guidance so everyone is on an equal footing. • MoJ could also review other jurisdictions for lessons on best practice exemption processes, and to enhance consistency.
1.15	Is the Minister of Justice the appropriate decision maker for exemptions under section 157, or should it be an operational decision maker such as the Secretary of Justice? Why or why not?	
1.16	Are the factors set out in section 157(3) appropriate?	
1.17	Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?	
1.18	Should the Act specify what applicants for exemptions under section 157 should provide? Should there be a simplified process when applying to renew an existing exemption?	
1.19	Should there be other avenues beyond judicial review for applicants if the Minister decides not to grant an exemption? If so, what could these avenues look like?	
1.20	Are there any other improvements that we could make to the exemptions function? For example, should the process be more formalised with a linear documentary application process?	
	(1) Institutional arrangements and stewardship – mitigating unintended consequences	
1.21	Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?	*Identity verification can pose challenges* The Amended Identity Verification Code of Practice (**IVCOP**) is restrictive for customers who, by virtue of age, financial limitations, or living or personal situations, are unable to obtain a passport or drivers' licence. Banks use their exemption handling processes where appropriate, however, we note this can lead to delays in account opening and can create frustration for customers. Increasing the available primary and secondary identification options within IVCOP, including for non-New Zealand residents, (for example, elevating the Kiwi Access card to a form of primary identification rather than requiring secondary identification and including
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?	

#	Question	Response
		a range of acceptable non-documentary forms of identity verification) should reduce reliance on exemption provisions. Specific options could be outlined for customers in certain circumstances (for example, accepting a Total Mobility Card). In addition to the above measures, existing identity documentation could be examined for opportunities to include richer data and therefore increase the ability of reporting entities to rely on the documents. For example, a SuperGold card with a photo and date of birth would be valuable for customer due diligence. Removing address verification (discussed below at item 4.50) would assist vulnerable customers who do not have a residential address to which documents can be addressed, or move accommodation regularly. This change would also, for example, help address the issues recently released prisoners face in obtaining bank accounts. *Challenges around exiting customers* A challenge in relation to the management of risks is the need to exit customers under certain circumstances – and reconciling the views between law enforcement and supervisory authorities on whether it is preferable to retain and monitor, or exit and prevent. A potential suggestion is allowing a defined basic banking service to be available to all customers, exempt from an obligation to exit (but importantly with the reporting entity retaining the ability to exit should the customer be deemed to be outside of risk appetite for other reasons). From an AML/CFT Act perspective, Section 37 could be amended to include exceptions to the obligation to terminate existing business relationships.
(1) Institutional arrangements and stewardship – the role of the private sector		
1.24	Can the Act do more to enable private sector collaboration and coordination, and if so, what?	NZBA supports the concept of private sector collaboration and coordination in principle. However, the implications of information sharing must be carefully considered, for example under the Privacy Act. It is very important that the Act sets out what is permitted, under what circumstances and for what explicit lawful purpose. For example, should a reporting entity be permitted to exit a customer upon receiving SAR-related
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?	

#	Question	Response
1.26	Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime?	information from another reporting entity, when the individual who is the subject of that SAR hasn't acted in a suspicious manner with the entity holding the current relationship? We suggest MoJ consider the approach recently introduced by AUSTRAC which involves the secondment of industry staff to supervisory authorities/law enforcement for the purposes of carrying out cross-sectoral risk analysis under a non-disclosure agreement.
1.27	Should the Act have a mechanism to enable feedback about the operation and performance of the Act on an ongoing basis? If so, what is the mechanism and how could it work?	In our view there are already sufficient forums to provide feedback, and we do not see benefit in introducing another mechanism. In our view benefits could be achieved through introducing mechanisms to ensure supervisors can quickly receive and act on industry feedback.
(1) Institutional arrangements and stewardship – powers and functions of AML/CFT agencies		
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?	In principle, NZBA supports the FIU being able to request information from businesses as required to discharge their obligations and support investigations. However, it is important that the necessary consultation happens between FIU and industry so that agreeable service-level agreements can be established, and relevant risks such as privacy risks are appropriately mitigated. The Act must cover the circumstances under which: • Information can be requested by the FIU; • The timelines within which reporting entities must facilitate the requests; • What information can be provided. The Act should be very prescriptive regarding instances when information can be shared, and information sharing outside of the parameters of the Act should not be permitted. We recommend this should only be progressed in consultation with the Privacy Commissioner.
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?	
1.30	Should the FIU be able to request information from businesses on an ongoing basis? Why or why not?	NZBA does not support a proposal enabling the FIU to request information from businesses on an ongoing basis. Reporting entities already have an obligation to conduct ongoing account monitoring of customer accounts, and to report any relevant suspicious activity within three days of forming suspicion. This proposal appears to extend this existing obligation to include 'real-time' reporting of suspicious activity. Such an obligation would be very resource intensive for banks to manage, as it would be a largely manual process. If MoJ wishes to progress this proposal, we would welcome a further and separate consultation.
1.31	If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?	

#	Question	Response
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?	We support the FIU having a power to freeze funds or transactions in instances where Police become aware of proceeds of crime and require time to complete an initial investigation and obtain a Court Order to restrain the funds. We do not think an asset freezing power should apply in instances of fraud or scams. In our experience, Police are not often involved in fraud or scams at the early stages when funds are still in an account. Banks have their own processes in place to help prevent and respond to scams and fraud.
1.33	How can we avoid potentially tipping off suspected criminals when the power is used?	There is, in our view, no way to freeze an account without a customer knowing. If the Police intend to freeze funds, it is appropriate that they should be prepared to engage directly with the individual/entity impacted. If a financial institution were to receive an inquiry from a customer about why their account was frozen, financial institutions should be able to refer the customer to the appropriate Police department for further information. The financial institution's role should be limited to freezing the account, with Police handling all communications as initiator of the action.
1.34	Should supervision of implementation of TFS fall within the scope of the AML/CFT regime? Why or why not?	Yes, in our view supervision of implementation of targeted financial sanctions (**TFS**) should fall within the scope of the AML/CFT regime. TFS is fundamental to the goal of countering financing of terrorism and is important for New Zealand's global reputation.
1.35	Which agency or agencies should be empowered to supervise, monitor, and enforce compliance with obligations to implement TFS? Why?	In our view, the supervising agency should have sufficient experience to understand TFS. We think that a dedicated agency which is able to develop its knowledge and experience is preferable to each of the current AML supervisors managing TFS with the entities they supervise.
(1) Institutional arrangements and stewardship - secondary legislation making powers		
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?	Our experience is that the process for issuing Codes of Practice can take some time. We support moving the decision making to the Chief Executives of the AML/CFT supervisors if doing so would result in a more efficient process. We also recommend including a requirement for supervisors to consult with industry when developing Codes of Practice.
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?	In our view, the ability to issue Codes of Practice should remain only with the supervisory authorities in order to separate regulation and enforcement, and mitigate the risk of inconsistent interpretation.
1.40	Are Codes of Practice a useful tool for businesses? If so, are there any additional topics that Codes of	We find Codes of Practise useful in providing direction to reporting entities, supplementing the risk-based approach underpinning the regime. However, it is important that they are consistently interpreted across the three supervisory authorities in

#	Question	Response
	Practice should focus on? What enhancements could be made to Codes of Practice?	their application. We also consider that Codes of Practice should incorporate the ability for reporting entities to make appropriate risk-based decisions, While we are overall supportive of a risk-based approach to AML/CFT, we would welcome the inclusion of the following topics in Codes of Practice to provide guidance in specific areas: • Establishing Beneficial Ownership • Ongoing Customer Due Diligence • High-risk customers and Enhanced Customer Due Diligence • Source of Wealth/Source of Funds • Monitoring and assurance (including system assurance) We believe it is important for industry to work with supervisors in developing 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?	In our view, demonstrating compliance through "equally effective means" is a very high bar and impacts the ability for reporting entities 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?	We consider that explanatory notes are a more flexible instrument for providing additional guidance than re-issuing a Code of Practice itself.
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?	As noted above in response to 1.38, moving the decision to operational decision makers would be beneficial if it reduces the time taken to make or amend the format of reports and forms required by the Act. However, there would need to be processes in place to ensure that decision makers understand the impact of their decisions on reporting entities.
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?	
(1) Institutional arrangements and stewardship – information sharing		
1.47	Would you support regulations being issued for a tightly constrained direct data access arrangement	NZBA does not support regulations being issued for a direct data access arrangement. The Privacy Act 2020 constrains banks' use and sharing of customer data. There are

#	Question	Response
	which enables specific government agencies to query intelligence the FIU holds? Why or why not?	limited circumstances where disclosure is permitted, and information sharing by the FIU must take this into consideration.
1.48	Are there any other privacy concerns that were not taken into consideration in the Privacy Impact Assessment 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?	
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?	
(1) Institutional arrangements – licensing and registration		
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?	In principle, NZBA supports a risk-based approach to licensing. However, large financial institutions are already subject to extensive licensing regimes and have mature AML programmes. Any licensing regime should reflect that banks are already subject to a number of other licensing regimes. In our view, licensing would be beneficial in the context of smaller reporting entities and those in higher-risk sectors where there may be concerns about exclusion. Such a licensing regime would provide comfort to banks that there is sufficient oversight and supervision, and that such industries have satisfied their requirements under the Act with a robust AML Programme. We recommend that licensing is also extended to auditors.
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?	

#	Question	Response
1.55	Should there also be an AML/CFT licensing regime in addition to a registration regime? Why or why not?	As noted in response to 4.133, we suggest a licensing regime and data retention scheme for virtual asset service providers and FinTech's would be useful to assist in understanding who has bought and sold virtual assets and the value of transactions. We also suggest that these requirements include an obligation on these entities to lodge suspicious activity reports in the same way as banks. Maintaining a general level of responsibility would still be appropriate, but financial inclusion concerns for this sector could be further addressed by expressly stating that reporting entities can primarily rely on that licencing / oversight by Supervisors, without being held responsible for activities of these organisations. We suggest referring to existing legislation setting out licensing and registration obligations for guidance if developing an AML licensing regime.
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?	
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?	
(2) Scope of the AML/CFT Act – challenges with existing terminology		

#	Question	Response
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?	In our view, all types of virtual asset service providers should be subject to AML/CFT obligations. With regard to tax-exempt non-profits and non-residential tax charities, an alternative could be to consider creating additional obligations on their registration with the Charities Register (or equivalent registration) and annual filing process, rather than including them in the AML/CFT Act.
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?	
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?	
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?	
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?	
(2) Scope of the AML/CFT Act – 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?	Please see our response below to question 2.48.
2.40	Should the exemption for internet auctions still apply, and are the settings correct in terms of a wholesale exclusion of all activities?	We think this exemption should still apply, within defined circumstances. Generally, internet auction providers and online marketplaces do not own the payment processor their website/business uses. In these circumstances, we do not believe that these

#	Question	Response
2.41	If it should continue to apply, should online marketplaces be within scope of the exemption?	businesses should be subject to additional AML/CFT obligations. However, it may be appropriate for these businesses to be subject to AML/CFT obligations where they own their payment processor. The scope of any obligations should cover a basic level of CDD. We understand there is an increased risk that online marketplaces can sell non-existent goods for money laundering or fraudulent purposes.
2.42	What risks do you see involving internet marketplaces or internet actions?	
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?	
(2) Scope of the AML/CFT Act – 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?	We suggest the following exemptions: • Additional Tier 1 (AT1) Perpetual Preference Shares issued by registered banks or special purpose vehicles under the Reserve Bank of New Zealand Capital Adequacy framework should be excluded from being "other repayable funds" under the definition of "financial institution" in the Act. • Part 13 of the Anti-Money Laundering and Countering Financing of Terrorism (Class Exemptions) Notice 2018 should be amended. The definition of "debt securities" should be expanded to include these AT1 capital instruments.
2.56	Should the AML/CFT Act define its territorial scope?	We consider that territorial scope definitions should remain in the Territorial Scope Guidance Note. However, we would welcome further clarity, for example, on what "carries on activities" means.
2.57	If so, how should the Act define a business or activity to be within the Act's territorial scope?	
(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?	*NZBA supports the current three supervisor model* NZBA considers that, overall, the current model with three supervisors works well. We make the following comments: • A challenge with this model is the time it can take for any triple branded publications to be released, given the complexities involved in all three supervisors 'signing off'. We note that this challenge may be mitigated if the decision-makers are changed from the Ministers to the Chief Executives of the Supervisors. We wonder if a further solution would be for guidance to address where there might be differences for different sectors, instead of all supervisors having to align on each point of the guidance. • There can sometimes be inconsistencies in approach and the standard different reporting entities are held to.
3.2	If it were to change, what supervisory model do you think would be more effective in a New Zealand context?	
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?	

#	Question	Response
		• Supervisors may be under-resourced relative to the job they are expected to do, which we note was also reflected as part of the Financial Action Task Force (FATF) Mutual Evaluation Report. *NZBA supports a risk-based approach to supervision* NZBA supports risk-based supervision in order to ensure resources are targeted towards those who have the greatest impact on financial stability, consumers, or where the risk of money laundering/financing terrorism is greatest. We recommend exploring a technological solution to support our AML supervisory approach, (perhaps something akin to the Probability Risk and Impact System model PRISM™ used in Ireland. We believe a tool to support risk-based supervision would be beneficial, particularly as we can only have a finite number of supervisors. Such a tool could be used to risk-assess the firms under supervision, and agree the frequency and intensity of supervision as warranted by the documented risks. Additionally, we suggest that supervisor onsite inspections should move away from an auditing exercise and focus on outcomes. Section 59 of the Act already requires reporting entities to carry out audits for compliance with their AML/CFT obligations, and our experience is that supervisor onsite inspections are often duplicative of these audits. We believe it would be more beneficial for onsite inspections to be a "deep dive" into particular areas (e.g. transaction monitoring), to assess the effectiveness of this process despite compliance with the Act.
(3) Supervision, regulation and enforcement – powers and functions		
3.5	Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why?	NZBA considers the powers and functions of the supervisors are broadly appropriate.
3.7	What are some advantages or disadvantages of remote onsite inspections?	In our view, the advantages of remote onsite inspections include: • Inspections can proceed safely during emergency/crisis events, including lockdowns and other COVID-19 restrictions. • Supervisors and reporting entities do not need to travel, which reduces both cost and carbon footprint. • Inspections could occur more frequently, contributing to a more efficient and less resource intensive inspection process.

#	Question	Response
		Some disadvantages of remote inspections include: • The risk of technology malfunction, for example, video call freezing may mean inspections are interrupted. • Cannot hand over physical files so all parties need to be prepared with relevant documentation. • Some people prefer face-to-face meetings to develop relationships.
3.8	Would virtual inspection options make supervision more efficient? What mechanisms would be required to make virtual inspections work?	As noted above, there are advantages and disadvantages associated with virtual inspections. In some instances, virtual inspections may make more sense, particularly during COVID-19.
3.9	Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient?	NZBA supports the introduction of a digital or electronic form. Additionally, we would welcome a notification model rather than an approval model. The extent to which the DBG is formed correctly, and the programme is demonstrating adequate coverage, can be subject to assessment via audits and onsite visits. In terms of the existing model, we note when a new member is joining an existing DBG, it is not clear that the member is required to include all the information requested under the "form for notification… of formation of a DBG". This should be clarified.
3.10	Should supervisors have an explicit role in approving or rejecting formation of a DBG? Why or why not?	Yes, supervisors should have an explicit role in approving or rejecting formation of a DBG. In our view, supervisors should only reject a DBG if it does not meet the required standards (e.g. not all members are eligible).
(3) Supervision, regulation and enforcement – regulating auditors, consultants and agents		
3.11	Should explicit standards for audits and auditors introduced? If so, what should those standards be and how could they be used to ensure audits are of higher quality?	In our view, it would be beneficial to introduce explicit standards for audits and auditors. These standards should prescribe what an audit must entail and the relevant skills/experience an auditor must have. We also suggest an additional guideline for those conducting the audit would be helpful, covering, for example, how long an audit should take, the level of scrutiny required, whether the audit will occur onsite or remotely, and whether it will involve a document review or process testing. In our view there is a broader piece of work required to educate reporting entities on auditing. Our experience is that reporting entities may not be familiar with the benefits of an audit, and the importance of your auditor having the requisite skills. Auditing should not be approached as a purely compliance exercise.
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?	

#	Question	Response
3.14	Should there be any protections for businesses which rely on audits, or liability for auditors who do not provide a satisfactory audit?	
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?	We do not consider it appropriate to specify the role of a consultant in legislation.
3.18	Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for?	Some of our members use agents to assist with their AML/CFT obligations. For example, a member may use an agent to collect customer due diligence information in the mortgage broker space and verify the information before sending it to the bank.
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?	Steps that a bank might take to ensure the appropriateness of their agent include background checks and customer due diligence on the agent and requiring the agent to sign an AML declaration.
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?	In our view, there would be benefit in regulating the steps a reporting entity must take to ensure that an agent is fit to carry out the role.
(3) Supervision, regulation and enforcement – offences and penalties		
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?	NZBA supports a penalty framework which is fair, transparent, proportionate and risk-based. The penalty regime should deter non-compliance and reward positive behaviour where appropriate. We suggest the introduction of a penalty framework which prescribes mitigating and aggravating factors. For example, severe customer impact, time without remedy and materiality of breach could contribute to a larger fine, while proactive engagement, self-reporting, lack of knowledge/intention could mitigate the severity of the fine. It's important that reporting entities' risk functions are able to assess regulatory risk exposure as accurately and clearly as possible for their Boards. We also consider that, in New Zealand, reputational damage is a significant deterrent. Increased use of public warnings rather than private warnings could enhance the penalty framework in the Act.
3.22	Would additional enforcement interventions, such as fines for non-compliance or enabling the restriction, suspension, or removal of a license or registration enable more proportionate, effective, and responsive enforcement?	
3.23	Are there any other changes we could make to enhance the penalty framework in the Act?	
3.24	Should the Act allow for higher penalties at the top end of seriousness to ensure sufficiently dissuasive penalties can be imposed for large businesses? If so, what should the penalties be?	

#	Question	Response
3.25	Would broadening the scope of civil sanctions to include directors and senior management support compliance outcomes? Should this include other employees?	We do not believe that broadening the scope of civil sanctions would significantly improve compliance outcomes. Our members already assign responsibility of managing AML/CFT risks at a senior management level, which ensures that senior managers are accountable for banks' AML/CFT programmes. In our view, civil sanctions would not create a difference in compliance outcomes. We also do not support extending the scope of civil sanctions to include other employees. This may create complexities, particularly for our overseas members whose employees do not reside in New Zealand.
3.27	Should compliance officers also be subject to sanctions or provided protection from sanctions when acting in good faith?	NZBA considers that compliance officers could also be subject to sanctions, provided they receive protection from sanctions when acting in good faith, or where escalation of issues to senior management are not appropriately acted on despite a compliance officer's best endeavours. Compliance officers have an important role to play, including setting compliance policies and procedures, monitoring, training and testing. In making decisions, compliance officers often rely on the facts and information provided to them by other business stakeholders. In addition, senior management approval is often required to take action on, or remediate, identified issues. Therefore, in order for the compliance function to continue to work effectively, compliance officers should not be subject to sanctions when acting in good faith in performing their duties, or where escalated issues are not resolved by senior management.
3.28	Should DIA have the power to apply to liquidate a business to recover penalties and costs obtained in proceedings undertaken under the Act?	In our view, DIA should have the same powers as the RBNZ and FMA as a supervisor under the Act.
(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?	There are a number of challenges associated with the CDD obligations. These include: • Address verification can be problematic due to the lack of documents physically mailed to customers. Electronic sources can be unreliable as the customer is often able to update an address themselves without verification. • Customers often provide recently expired identity verification, particularly in the context of the COVID-19 pandemic.

#	Question	Response
		• There are varying degrees of due diligence required for different AML/CFT obligations. For example, the level of due diligence required at on-boarding is higher than the level required to submit a PTR. • The three-month certification period poses issues for customers, who often have access to documents that have previously been 'certified' but not in the last three months. • There can be inconsistencies between the certification rules in New Zealand and overseas, so we sometimes see overseas customers provide documentation that is legitimately certified in their country but not in New Zealand. • It can be challenging to obtain source of wealth/funds for every trust, particularly lower risk family trusts. • It is unclear what exactly is required to verify source of wealth/funds. Guidance would be helpful to clarify how far back reporting entities have to trace, and whether both source of wealth and source of funds need to be identified. We note also that in some instances (e.g. lending), customers may not have 'wealth' or 'funds', so it is challenging to collect and verify this information. • Customers that are entities can pose additional challenges. For example, there are no prescribed requirements around evidencing a customer's structure, and customers can be unwilling to share these details (particularly in the case of trusts). Lack of prescription also makes syndicated lending arrangements problematic, as reporting entities must apply the highest common denominator and/or utilise exemption handling procedures due to variances in risk-based approaches between the syndicated members. • New Zealand's CDD obligations are often more restrictive than those of other jurisdictions our members commonly deal with (e.g. Australia). The requirements can be complex and require navigation of multiple legislative sources. • The IVCOP offers only a minimal range of acceptable identity verification documents for overseas residents, which has materially impacted branches of overseas banks and locally incorporated banks with a material non-resident client base. This also includes persons acting on behalf of a customer who may be based outside New Zealand, but who are acting on behalf of locally incorporated customer entities. • The closure or offboarding of low risk but high complexity customers can be challenging. For example, a home loan customer that does not provide the

#	Question	Response

		requisite CDD/ECDD documents must be offboarded under section 37, but it is very complex to close a home loan customer.
		
		We make the following suggestions:
		• **Removal of Address Verification:** While address collection is useful in contributing to the assessment of jurisdictional risk and the prevention of fraud, the current obligation to verify such information is not fit for purpose (noting that residential address can and does change on short or no notice) and can have a disproportionate impact on customers. We recommend that the obligation to obtain address verification be removed from the CDD section of the Act in all circumstances (including high-risk customers). The Act could retain a requirement for reporting entities to collect this information where available, but not have to verify it.
		• **ECDD on Trusts**: There are different types of trusts each with varying degrees of risk exposure from a money laundering or terrorist financing perspective. As such, the obligation to apply ECDD on Trusts should be amended to reflect that nuance. Entities should be able to risk-rate trusts based on the different types, and apply CDD measures according to the levels of risk involved.
		• **Beneficial Ownership:** we recommend that consideration of beneficial ownership is more holistic, in line with EU's Beneficial Ownership regime. We suggest the following changes:
		  ○ Establish a central public Beneficial Ownership Register (for Entities) and a Trust Register
		  ○ Require all companies to create their own individual Beneficial Ownership Registers and to keep the public register updated as details change
		  ○ Define beneficial ownership for the purposes of all entity types within the legislation itself
		  ○ Establish a trust register and require trustees to create beneficial ownership registers for each trust and keep the public register up-to-date.

#	Question	Response
		○ Include specific obligations on what it required vis-à-vis beneficial ownership verification on an ongoing basis • **OCDD Triggers:** Include baseline instances in the Act where a review of CDD needs to be performed on existing customers. Entities can then do more as warranted by their own risk assessments. • **Reliance and Outsourcing:** Simplify the circumstances under which a reporting entity can rely on external entities to perform CDD on their behalf – especially where the external entity is duly authorised and regulated. • **LMI/SMI Exemption:** Disestablish the intermediaries exemptions and incorporate this as part of the simplification of reliance and outsourcing. Remove the concept of POWBATIC and the obligation for reporting entities to perform CDD on them – instead allowing for reliance on the CDD performed by the intermediary who has the relationship with the underlying customer. • **MSB and Payment Intermediaries Due Diligence:** Introduce prescribed due diligence requirements on MSBs and Payment Intermediaries (in line with requirements which currently apply to correspondent banking relationships) • **RMA Due Diligence:** Confirm whether any due diligence obligations should extend to RMAs, the type of due diligence to be conducted and the circumstances under which they should be conducted. • **Additional Guidance:** It is recommended that additional guidance be provided on CDD with regards to the following circumstances: ○ Minors ○ Vulnerable situations (care homes, homeless etc.) ○ Who the customer is and the level of due diligence required when the client is a fund e.g. fixed unit trusts, mutual/corporate or retail funds, trust funds or investment funds. • **Expired ID Documents:** We would welcome a formal position on the use of expired documentation in verifying identity. • **Electronic ID Verification:** We recommend that digital ID verification be supported and encouraged – leveraging the technologies that are available and that the public sources of information be leveraged to support general technological innovation.

#	Question	Response
		○ The Digital Identity Services Trust Framework Bill aims to promote the provision of secure and trusted digital identity services that meet essential minimum requirements for security, privacy, identification management and interoperability, aims which we strongly support. It is also important that the development of digital ID framework legislation has, as a baseline, alignment with AML/CFT and Identity Verification requirements, and be capable of being relied on for the purposes of fulfilling these requirements. Consideration should also be given to, and possible alignment made with, overseas generally accepted electronic/digital verification practices. This will enable greater buy-in from the private sector and in turn should ensure that wider consumer benefits are realised. ○ In order to more easily meet the requirements of section 15(e) of Part 3 of the IVCOP and given the incidence of fraudulent drivers licences, it would be helpful if Section 200 of the Land Transport Act 1998 could be amended to enable an original photo to be made available when completing an NZTA check. ○ Given the volume of customers who utilise preferred names / English names and other challenges such as spelling mistakes due to data entry errors, hyphenation, name order being different in different cultures and so forth, it can be quite difficult in many cases (particularly for a new to country customer) to successfully obtain a matching customer name verification from two independent and reliable sources - and we question whether the requirement for a second independent and reliable match clearly reduces the risk when there are other requirements such as section 17(e) (linking the customer to the claimed identity). We request that consideration be given to: ▪ Removal of the requirement in section 15(a) for two independent and reliable matching electronic sources; ▪ Further clarity on whether the expectation for "matching" requires a perfect / identical match or whether there is some tolerance

#	Question	Response
		permissible (particularly when the DOB also matches across 2 sources); or ▪ The requirement is modified to indicate that the customer's identity (rather than specifically name) must be verified from two independent and reliable (but not matching) sources - so that equally effective and acceptable measures could be available to confirm a secondary existence of the customer's identity without specifically the name needing to match across two electronic sources. • **Information Sharing**: we recommend consideration be given to the advantages of departments sharing information with reporting entities to support reporting entities to conduct compliant CDD and reduce identity theft. Examples include: o NZTA supplying a photo when confirming identity matches, and o DIA/Immigration enabling the querying of immigration data for non-New Zealanders. It would also be helpful to clarify the position relating to guarantors and other security providers for a customer's lending arrangements, but who have no other relationship with the reporting entity. We would welcome an enhanced definition of what constitutes "complex".
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?	NZBA supports a more prescriptive definition of customer, and is of the view that the definition should be as simple as possible. In our view this definition would be particularly useful for more complex structures, such as managed funds, where there are various parties such as the trustee, fund manager and custodian, making it difficult to determine where the focus of the "customer" enquiries should be.
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?	

#	Question	Response
4.5	Do you anticipate that there would be any benefits or additional challenges from a more prescriptive approach being taken?	
4.9	Are the prescribed points where CDD must be conducted clear and appropriate? If not, how could we improve them?	NZBA considers the existing drafting is reasonably clear, with the exception of existing customers. We would welcome greater clarity around what is actually required with existing customers.
4.10	For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear?	We would welcome an enhanced definition of what constitutes a "complex" transaction.
4.11	Should CDD be required in all instances where suspicions arise?	We do not support CDD being mandated in all instances where suspicions arise. Staff need to balance the CDD requirements with the "tipping off" provisions, and a conflict between these two obligations may arise if CDD is mandated in all instances where suspicions arise. Banks can and do encourage staff to obtain CDD information, but as "suspicion" is subjective, it will be difficult to mandate and conduct assurance over.
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?	
4.18	Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?	NZBA considers that the requirement to verify residential address is no longer appropriate. Given the decline in physical mail, we find it is very difficult for some customers to provide this verification and can lead to financial exclusion. We also note that it can be challenging to verify source of funds/wealth for all trusts, and suggest a risk-based approach to this requirement would be sensible. We consider that clarification around the verification requirements for nominee shareholders would be beneficial. For example, if nominee shareholders are minority shareholders, are reporting entities still obliged to carry out enhanced customer due diligence.
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?	
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?	NZBA understands that some of its members, including overseas branches which are subject to other AML/CFT regulatory regimes, already obtain this information. If onboarding a company, many of our members will obtain the company extract from the Companies Office, and may also look at the company's constitutional documents. If the ultimate owner of the company was an offshore company, our members would typically

#	Question	Response
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?	request a certificate of incorporation. For trusts, our members typically obtain a copy of the Trust Deed.
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?	
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?	We would welcome clearer guidance on all aspects of ECDD. We find this is a difficult requirement to navigate and the regime would benefit from further prescription/explanation, either in guidance or regulations. It would be beneficial for any regulations to differentiate between the requirements for new and legacy/existing trusts. Additionally, it would be helpful to clarify whether banks are able to rely on existing information they hold as a source of verification.
4.27	Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds?	We anticipate that any further requirements in this area would increase the time to onboard customers.
4.30	Have you encountered issues with the definition of a beneficial owner? If so, what about the definition was unclear or problematic?	The 'third limb' or 'person on whose behalf a transaction is conducted' element of beneficial ownership is challenging. This needs to be removed or made explicit that it is in relation to individual customers only, not non-individual customers
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?	We understand that most of our members already focus on identifying the 'ultimate' beneficial owners. We would welcome clarification or guidance on what level of verification is required for intermediate shareholders (i.e. those between the direct customer and the ultimate shareholder). For example, are businesses required to obtain proof of existence for an intermediate company, or is it sufficient to rely on a structure chart?
4.33	To what extent are you focusing beneficial ownership checks on the 'ultimate' beneficial owner, even though it is not strictly required?	
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?	We would support this regulation. We agree that issuing this regulation would mean Regulation 24 would no longer be required. We note that the reference to 'control' can be challenging. We would welcome further guidance on how we could identify 'control', and the necessary verification steps. We

#	Question	Response
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?	note the existing guidance on beneficial ownership, but support further guidance on what control means.
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?	
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?	Again, we note that identifying the person who "controls" a legal person can be challenging and we find ownership easier to identify. We do not support regulations which mandate an approach consistent with FATF standards for identifying beneficial owner of a legal person, particularly if that guidance stated that a senior managing official should be identified as the beneficial owner where no persons can otherwise be identified.
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?	
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?	Our members already identify the settlor, trustee, protector and other identified persons exercising effective control over the trust or legal arrangement. Any regulations would need to include recognition that not all trusts/legal arrangements will have each of these roles in place. Additionally, we note that there are situations where these roles will not exercise any control or influence over the trust/legal arrangement, so the regulations would need to be sufficiently broad to capture those exercising control. We also note that, in the case of trusts, requiring verification for the settlor can sometimes be difficult or not relevant. For example, some settlors will no longer be alive,
4.43	Would there be an impact on your compliance costs by mandating that this process be applied? If so, what is the impact?	

#	Question	Response
		or may no longer have anything to do with the trust (e.g. if a lawyer or accountant established the trust but have no ongoing role).
4.45	Do you encounter any challenges with using IVCOP? If so, what are they and how could they be resolved?	We find that the IVCOP is very prescriptive and as a result, our members frequently use an exception handling process. We recommend increasing the range of accepted forms of ID and the accepted combinations of forms. We would welcome: • The inclusion of international/overseas identification e.g. drivers' licences if these could be appropriately controlled and risks mitigated – for example, drivers' licences from low risk or pre-specified countries. • Exploring the possibility to elevate the status of a KiwiAccess card to a form of primary identification. • Exploring the addition of a "Verifying Officer" provision. • Expanding the definition of "Bank statement" in the IDVCOP to clarify that this encompasses other documents that can be issued by a bank (for example, the letter that accompanies the issuance of a new debit or credit card). • Including in the IVCOP the definition of "Government agency" and consider whether this should be expanded to include local government. In relation to Part 3 of the IVCOP and the July 2021 Explanatory Note: Electronic Identity Verification Guideline, we would welcome more guidance on the expected independent and reliable sources that should be used for identity verification of individuals that are not located in New Zealand. The Electronic Identity Verification Guideline currently provides guidance on the expected sources to verify the name and date of birth of an individual that is in New Zealand (section 13 of the Electronic Identity Verification Guideline). However, the guideline is silent on the expected sources for verification of individuals located overseas. We would welcome more guidance on the expectation for overseas electronic identity verification. We do not see benefit to changing the standards for high-risk customers, particularly if we already receive an individual's passport. We note that currently our members verify the name and DOB for high-risk customers. Not directly related to the questions posed but related to the IDVCOP is the issue of certification of documents; it is unclear what the expectations are for documents other
4.46	Is the approach in IVCOP clear and appropriate?	
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 highrisk 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?	

#	Question	Response
		than ID documents. The IVCOP requires that ID be certified but does not state what the expectations/requirements are around other documents such as trust deeds, SoW/F documents etc. Finally, in our view remediating incorrectly certified documents takes up a disproportionate amount of time. Of particular note is the requirement for "is a true likeness", or equivalent statement. This is frequently omitted by overseas certifiers in particular. The list of acceptable overseas certifiers is also restrictive and doesn't align with global standards. Inclusion of certification (or face to face verification) by employees of overseas affiliates of a NZ reporting entity would also be welcomed (and if deemed necessary, subject to regulation under a jurisdiction with sufficient AML/CFT systems in place). It may also be an option to allow risk acceptance of certification wording for overseas certified documents where this differs to the wording prescribed in the IVCOP.
4.50	What challenges have you faced with verification of address information? What have been the impacts of those challenges?	Address verification is one of the primary challenges our members face in relation to this Act. We strongly support removal of address verification as a requirement in the Act as it is unclear what (if any) material benefit is gained from doing so. Some of the reasons address verification poses such a challenge include: • There is not a clear list of acceptable address options, which can lead to confusion for frontline staff. • Customers can face financial exclusion if they are not able to verify their address. Customers in vulnerable circumstances are most often impacted, including those in transient housing. • A large number of New Zealanders live in rental accommodation and shared living arrangements where only a "head tenant" is listed on the tenancy agreement and other tenants are not able to verify their address. • Prisoners who are about to be released, or are recently released, are not able to provide address information and find it very difficult to open bank accounts. • People often live at home with their parents and are not able to provide the accepted documentation. We do not see a benefit in address verification that corresponds to the difficulties. Our members would likely still seek to collect address information where it is available for a range of reasons, but in our view there is no additional benefit found in verifying this information.
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?	

#	Question	Response
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?	We note that many of these steps fall under "Nature and Purpose", so reporting entities are likely already taking these steps. We would welcome a Code of Practice which outlines the additional measures that businesses can take as part of ECDD. We consider that industry consultation would be important to ensure that the Code is operationally manageable.
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?	
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?	In our view, simplified CDD should be extended to all AML-licensed or regulated entities in low-risk jurisdictions. It is our understanding that New Zealand's current approach does not align with global practices. We would welcome further guidance on the scope of individuals who are "persons acting on behalf of a customer". We note the "acting on behalf of a customer fact sheet", and that it would benefit from additional guidance that details who the supervisors define as a person acting on behalf of a customer, when offering a client a product such as online banking.
4.57	Should we issue regulations to allow employees to be delegated by a senior manager without triggering CDD in each circumstance? Why?	
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?	We support removing the requirement for ECDD to be conducted for all trusts or vehicles holding personal assets. In our experience most trusts/vehicles holding personal assets are not high-risk, and this requirement can be challenging. As an alternative, we recommend providing guidance or regulations outlining "red flags" that might indicate a high-risk trust, and when reporting entities are required to carry out ECDD.
4.59	If we removed this requirement, what further guidance would need to be provided to enable businesses to appropriately identify high risks trusts and conduct enhanced CDD?	
4.60	Should high-risk categories of trusts which require enhanced CDD be identified in regulation or legislation? If so, what sorts of trusts would fall into this category?	
4.61	Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?	We find ongoing CDD requirements can be unclear, and there is limited guidance to assist with interpreting and understanding compliance expectations. NZBA supports greater clarity in the legislation, and welcomes an ongoing CDD Code of Practice to assist with clarifying these obligations.

#	Question	Response
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?	From an Ongoing CDD perspective, our members typically treat the account monitoring and CDD components of section 31 as separate processes. CDD information may be checked as part of account monitoring, but is not updated. We consider that the legislative objectives are achieved by the current practice of updating CDD information as part of OCDD. In our view, reviewing and updating CDD as part of account monitoring would unnecessarily increase the compliance burden and costs. We would support the introduction of more clearly defined triggers for when CDD must be reviewed and updated. Additionally, we consider that greater clarity on what information must be checked and updated during an ongoing CDD review would be beneficial (for example, whether nature and purpose should be reviewed and updated, or whether it could be inferred from transactional history). We see clarity on these issues as more urgent than frequency prescription. Less urgent, but still helpful, would be clarity regarding expired identity documentation, and whether this needs to be refreshed as part of ongoing CDD.
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?	
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?	Our members consider the customer profile as a whole, rather than account behaviour only. This consideration includes looking at open-source information, IP addresses, previous ML/TF investigations undertaken, lending applications, customer communications, etc. We do not consider regulations necessary, but guidance could be helpful.
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?	
(4) Preventative measures – conducting CDD on existing (pre-Act) customers		
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?	We find the current wording ambiguous and note that detailed guidance would clarify the requirements.
(4) Preventative measures – 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	We note that there can be a conflict between meeting obligations for ECDD/SAR and the obligation to avoid tipping off customers. Our members use their discretion and

#	Question	Response
	determine whether conducting CDD or enhanced CDD may tip off a customer?	judgement to manage this conflict on a case-by-case basis. If they decide not to conduct ECDD for a SAR, they have a clearly defined escalation process. We support greater clarity in the legislation, including further detail on how to balance these sometimes conflicting obligations. We suggest referring to AUSTRAC's work in this space, who have issued guidance setting out the obligations on reporting entities in relation to tipping off, as well as examples of how to comply. We also see some confusion with the three-day reporting timeframe, specifically, when the three-day period commences. We would welcome clarity on this point. If the 3 days commences at the point of transaction, or when an internal SAR is submitted, then obtaining ECDD within this timeframe is generally not possible so ECDD is always obtained after the SAR is submitted.
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?	
(4) Preventative measures – record keeping		
4.76	Do you have any challenges with complying with your record keeping obligations? How could we address those challenges?	We support clarity in relation to the record keeping obligations. If prescribing retention periods, it is important to consider reporting entities' other domestic and international retention obligations.
4.77	Are there any other records we should require businesses to keep, depending on the nature of their business?	
4.78	Does the exemption from keeping records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold hinder reconstruction of transactions? If so, should the exemption be modified or removed?	
(4) Preventative Measures – 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?	Our members do not have any specific challenges to call out, but note that this obligation can be time-consuming, with a lot of time spent working on "false positives" i.e., a person who turns out not to be a PEP.

#	Question	Response
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?	We support expanding the definition of 'politically exposed person' to include domestic PEPs. Any change will require a clear definition so reporting entities know which level of official will be captured as a PEP. We suggest local government officials should not be included; the obligation should be limited to central government. We also suggest limiting the obligation to those who are elected, rather than extending it to political candidates and close associates. We suggest establishing a centralised list of prominent public functions to ensure that ECDD measures on PEPs are only applied in intended instances.
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?	It is difficult to estimate cost incurred, but our members suggest these changes could result in a doubling of the current resources allocated to managing PEP customers.
4.85	How do you currently treat customers who were once PEPs?	We support a risk-based approach to determine whether a customer who no longer occupies a public function should still be treated as a PEP. In our view the current prescriptive timeframe should be removed; influence does not necessarily expire after a certain period outside of office.
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?	
4.88	What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP?	Our members screen against lists from third-party vendors, the FIU and overseas governments. In our view, using commercial lists is an effective and efficient way to determine whether a customer is a foreign PEP. In larger organisations, it would be very difficult to manage the customer base without screening against commercial lists. We consider that the Act's use of "take reasonable steps" is clear. In our view, the Act should not mandate that businesses undertake the necessary checks before the relationship is established. Such a mandate may be challenging in some instances in the retail sector, and bank processes would likely need to change to reduce "false positive" identification of PEPs, increasing the risk that some PEPs are missed. We also consider it would be very challenging to complete ECDD before the 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?	
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?	

#	Question	Response
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?	is established, as a customer would likely be reluctant to provide all the required information before a business relationship is established. With regards to occasional activity or transactions, screening 'before' the activity or transactions is not going to be feasible, these are 'over the counter' transactions that happen real time and cannot be held up while a PEP check is completed.
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?	In our view, domestic and international organisation PEPs should be treated the same. Different rules may lead to confusion. Our members take a range of steps to help mitigate the risk of customers who are PEPs, including: • Specific transaction monitoring rules • Periodic reviews • Senior manager approval required for establishing the relationship • Source of Wealth and Source of Funds procedures carried out.
4.93	If we include domestic PEPs and PEPs from international organisations within scope of the Act, should the Act allow for business to take reasonable steps, according to the level of risk involved, to determine whether a customer or beneficial owner is a domestic or international organisation PEP?	
4.94	What would the cost implications of including domestic PEPs and PEPs from international organisations be for your business or sector?	
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?	
4.97	What steps do you currently take to mitigate the risks of customers who are PEPs?	
4.98	Should the Act mandate businesses take the necessary mitigation steps the FATF expects for all foreign PEPs, and, if domestic or international organisation PEPs are included within scope, where they present higher risks?	

#	Question	Response
4.99	What would be the cost implications of requiring businesses to take further steps to mitigate the risks of customers who are PEPs?	
(4) Preventative measures – implementation of targeted financial sanctions		
4.100	Should businesses be required to assess their exposure to designated individuals or entities?	Some of our members already have a sanctions programme in place that screens for possible exposure to sanctioned individuals or entities. We support the inclusion of targeted financial sanctions within a reporting entity's overall compliance programme and make the following comments: • The sanctions programme should be able to standalone from the AML/CFT Act. • The requirements should be clearly defined so they can be assessed accordingly and subject to a consistent level of regulatory scrutiny by supervisors. • We recommend the introduction of a 'sanctions risk assessment' with specific guidance on what to include. • We recommend the introduction of a requirement to assess the sanctions risk associated with products, channels and technologies. • We recommend there be one supervisor responsible for oversight of sanctions compliance to ensure consistent interpretation of obligations.
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?	
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?	Sanctions and AML go hand-in-hand, so we consider that it makes sense for sanctions to at least sit alongside the AML Programme, if not directly included in it. If it forms part of an AML programme then it has to be part of audits and inspections, subject to supervision.
4.104	What support would businesses need to develop such policies, procedures, and controls?	
4.105	How should businesses receive timely updates to sanctions lists?	We understand that large entities will use commercial lists and rely on third-party vendors to update the lists in a timely manner.
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?	

#	Question	Response
4.108	Do you currently screen for customers and transactions involving designated persons and entities? If so, what is the process that you follow?	Most of our members have automated screening of customers, employees and all international payments. Screening occurs automatically and any alerts are manually reviewed. There is an escalation process in place for high-risk alerts, and any true matches are dealt with accordingly by either closing accounts, declining transactions or exiting employees. There is unlikely to be a significant cost implication for the reporting entities that already follow the above process, but we expect it may be costly for reporting entities who are not already carrying out this process.
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?	
4.113	Should the government provide assurance to businesses that have frozen assets that the actions taken are appropriate?	Yes, we consider that government assurance would be beneficial in this instance.
(4) Preventative measures – 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?	As noted under 4.1 above, clarification or confirmation, in the legislation around whether any due diligence obligations should extend to RMAs and the circumstances under which they would be beneficial.
(4) Preventative measures – money or value transfer service providers		
4.117	If you are an MVTS provider which uses agents, how do you currently maintain visibility of how many agents you have?	We consider that MVTS providers should be required to maintain a current list of their agents and be responsible for the oversight of their agents, and this should include formally documented regular reviews.
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)?	
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?	Yes, as above.

#	Question	Response
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?	Yes, we support regulations being issued to explicitly require MVTS providers to monitor and manage their agents for compliance with their AML/CFT programme. Obligations on MVTS providers should be consistent with obligations on other reporting entities, for example, banks cannot outsource their AML risk to their agents.
4.124	Who should be responsible for the AML/CFT compliance for sub-agents for MVTS providers which use a multi-layer approach? Should it be the MVTS provider, the master agent, or both?	It makes sense for both the MVTS provider and the Master Agent to be responsible.
(4) Preventative measures – new 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?	We recommend introducing an explicit requirement to perform a risk assessment in relation to new products or technologies launched. We suggest including this in regulations and supported by guidance. Our members already conduct risk assessments prior to the launch of any new product or service or channel and mitigate identified risks. The cost implications would be minimal for the reporting entities who already carry out this work.
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?	
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?	
(4) Preventative measures – 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	We would find it beneficial for supervisors to assign a risk grading at a product level for virtual assets (e.g. transfers between a bank's internal entities would be low-risk while transfers outside may be higher risk).

#	Question	Response
	that we should provide to assist them with complying with their obligations?	We would also welcome further guidance on the expected treatment and monitoring of virtual asset service providers who are third parties involved in cross border wire transfers. We suggest a licensing regime and data retention scheme for virtual asset service providers would be useful to assist in understanding who has bought and sold virtual assets and the value of transactions.
4.134	Should we set specific thresholds for occasional transactions for virtual asset service providers? Why or why not?	Yes, we believe a specific threshold will help in ensuring the focus is on materiality of the transfers.
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?	We suggest $1,000 is more appropriate as it aligns with the PTR threshold.
4.137	Should we issue regulations to declare that transfers of virtual assets to be cross-border wire transfers? Why or why not?	If the value is being transferred internationally, in our view it should be treated as a cross-border wire transfer. Additionally, crypto-currency providers should have the same IFT reporting obligations as a bank if any of the transfers are cross-border wire transfers.
4.138	Would there be any challenges with taking this approach? How could we address those challenges?	We believe a challenge will be the quality of the cross-border wire transfer data. Virtual assets can be compared with securities instead of payments and therefore, we suggest any applicable regulation is similar to regulation that applies to securities exchanges.
(4) Preventative measures – wire transfers		
4.139	What challenges have you encountered with the definitions involved in a wire transfer, including international wire transfers?	Further clarity on the definition of international wire transfers would assist in simplifying the complexity of reporting these transactions. For example, it is difficult to interpret and apply the exclusion relating to transfers and settlements between financial institutions where both the originator and beneficiary are both financial institutions or reporting entities acting on their own behalf. It is hard to align that exclusion with the current legislated definitions of "ordering institution" and "beneficiary institution", and then determine whether the exclusion applies only when those two parties are involved in direct settlements and transfers, or whether it also applies when those parties are facilitating transfers or settlements for customers who are themselves financial institutions that are transferring or settling funds to another financial institution.
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?	

#	Question	Response
		In addition, based on current definitions there are operational difficulties in NZ beneficiary banks identifying domestically settled international payments that may be subject to PTR reporting requirements. We also note that definitions may need to be modernised to reflect the variety of transfer methods now available, for example crypto exchanges or intermediary institutions.
4.142	What information, if any, do you currently provide when conducting wire transfers below NZD 1000?	Our members' policies typically do not differentiate the information provided based on value. The same level of originator and beneficiary details are provided, irrespective of transaction value.
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?	This would be unlikely to materially affect our members' ability to monitor transactions, and to the best of our knowledge we are also unaware of any specific instances where collecting this information for a transaction under NZD$1,000 would have changed the outcome of any investigation or report.
4.144	What would be the cost implications from requiring specific information be collected for and accompany wire transfers of less than NZD 1000?	We believe the main cost implications would come from additional staff required to engage the originating bank for further information. The level of cost incurred will vary depending on the size of the reporting entity.
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?	In the case of an outward transfer, our members will contact their customer to obtain further details. If the transfer is inward and contains insufficient information, we understand our members will process the transfer as normal. Payments over the $1,000.00 threshold are held and remitter banks are contacted via SWIFT to obtain missing details. If details are not received, the payment will be returned to the sender.
4.148	When acting as an intermediary institution, what do you currently do with information about the originator and beneficiary?	We understand that some of our members retain the information provided.
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?	We understand that many of our members screen all international transfers to ensure sufficient information is captured. Payments with beneficiary names under a certain character limit, or with key words such as "PO" or "Box" are examples of payments that would get flagged as potentially having insufficient beneficiary details and would be then subject to manual review.
4.154	Should we issue regulations requiring beneficiary institutions to take reasonable measures, which may include post-event or real time monitoring, to identify	We support issuing regulations as that would bring other institutions involved with sending or receiving funds from overseas up to the level of compliance currently required of banks and financial institutions.

#	Question	Response
	international wire transfers that lack the required originator or beneficiary information?	It will be helpful to clarify the definition of "complete beneficiary information" before applying any monitoring.
4.155	What would be the cost implications from requiring beneficiary institutions to take these steps?	In our view there would be minimal cost implications for banks and financial institutions that will already have systems in place.
(4) Preventative measures – 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?	Our members find the current requirements complex, particularly given the nature of payments infrastructure. The requirements contain exclusions (by value, by transaction type) which are challenging to code in an automated reporting system. We would welcome a Code of Practice or more specific guidance to provide clarity. Our members find the topics below particularly complex and would welcome a Code or guidance: • **Trade finance**. Transactions facilitated via MT202s, and where funds transfers are not directly sent internationally, instead deals are made between banks and their customers in 2 separate jurisdictions in order to facilitate a trade. • **Instances where MT202s (or other similar message types) are used to facilitate funds transfers on behalf of an underlying customer**. Banks have very limited ability to control messages sent to them. There are payments that might meet the SWIFT definition for use of a MT202 but not the wire transfer exclusion for a 'financial institution to financial institution' settlements where both parties are acting on their own behalf, which are complex to identify and code for. MT202s may not contain all the same information and so may not fit the PTR schema requirements. • **Credit card to credit card payments that have a cross-border element**, which are not currently reported as long as the payment contains a credit card number. Credit card companies do not have the same obligations. • **Situations where financial institutions and DNFPBs are customers of other reporting entities and either initiate or receive funds on behalf of a third party**. It is unclear in these instances who has the obligation to report, who the ordering institution is and who the beneficiary institution is. • **Instances where one bank considers it is acting as an intermediary institution, whereas another bank considers the receipt of funds from that bank to be a domestic wire transfer with no intermediary institution**
4.157	Have you encountered any challenges in complying with your PTR obligations? What are those challenges and how could we resolve them?	
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?	

#	Question	Response
		involved. Our members find that visibility of information for domestically settled wire transfers can be an issue. Additionally, the definition of intermediary needs to be clearer and consideration given to technical complexities associated with identification of such payment when these are settled via domestic payments systems. We would also welcome standardisation on how information should be provided to the next party in the payment transaction chain. • **Bulk or batched international wire transfers that are processed via SWIFT (MT103 or MT202), but underlying payment instructions are sent outside of SWIFT and payments could be considered as domestic payments**. • **Payments between 2 NZ banks in a foreign currency but offshore intermediary is used to facilitate the FX requirements**. It is unclear to us whether these payments are intended to be reported and whether they have any intelligence value. • **Incoming international wire transfers to reporting entities through intermediaries** – Intermediary banks with correspondent banking relationships facilitate international payments for domestic beneficiary banks, who don't have correspondent relationships. The beneficiary bank is reliant on PTR information being provided accurately and in a timely manner by the intermediary bank to meet PTR obligations. There is not requirement for the intermediary banks to provide sufficient or timely information for PTR purposes. • **Cross-border corporate funds sweeps as part of a corporate's treasury management.** It is unclear to us what the reporting expectations are here. • **ISO20022 implications for PTR**. Regulation and guidance need to align to new industry payment structures. • **Nostro account settlements**. It is unclear to us what the reporting expectations are here. We also note that PTR obligations are relatively complex compared to other obligations in the Act. This leads to a disproportionate focus on compliance rather than a risk-based approach. Potential options to address this include defences, reasonableness measures or materiality references.

#	Question	Response
4.160	Should non-bank financial institutions (other than MVTS providers) and DNFBPs be required to report PTRs for international fund transfers?	We support requiring non-bank financial institutions to report PTRs where they hold information on the ultimate originator/beneficiary, but would not want this requirement to further increase the reporting burden for our members.
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?	
4.166	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?	Our members have encountered some challenges with the 10-working day timeframe. When banks have automated PTR reporting, all exceptions must be handled manually. Additionally, technology incidents with a downstream impact on PTR reporting are sometimes discovered several days into the 10-day period. In our view a 20-working day timeframe would be more appropriate.
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?	In our view a lower threshold may be sensible but would have significant cost implications for some reporting entities that may not be commensurate with the risk. However, we submit that the current lack of clarity with PTRs (outlined above) needs to be resolved before making any change. We expect there would be significant testing and assurance work required prior to implementation of any changes to PTR requirements, and we estimate that at least 12 months would be required to implement the change, which will include the necessary technology development and staff training. We note that a longer period (18 months) may be required depending on the complexity of the changes. We note that consideration will need to given to the impact that lowering the threshold will have on Smart ATMs and the limits allowed to be deposited via those channels.
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?	
(4) Preventative measures – reliance on third parties		
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?	We support removing this approach as it does not align with FATF and it is not being utilised currently.
(4) Preventative measures – internal policies, procedures and controls		
4.187	Are the minimum requirements set out still appropriate? Are there other requirements that	We consider these requirements still appropriate.

#	Question	Response
	should be prescribed, or requirements that should be clarified?	
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?	We do not support mandating that the compliance officer be at senior management level, based on the current definition. This requirement might have unintended consequences for smaller firms. At larger firms it is likely the senior manager wouldn't focus on AML, rather, it would be part of their wider remit and they would delegate responsibility. In our view the appropriate requirement is that the compliance officer must be sufficiently experienced, resourced and senior within the firm to discharge their obligations.
4.189	Should the Act clarify that compliance officers must be natural persons, to avoid legal persons being appointed as compliance officers?	We support the Act clarifying that compliance officers must be natural persons.
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?	We would welcome guidance on this topic but do not consider it appropriate to mandate expectations.
4.193	Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system?	Yes, we support the legislation stating that the purpose of an independent audit is to test the effectiveness of a business's AML/CFT system.
(4) Preventative measures – high-risk countries		
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?	We support a risk-based approach continuing in relation to high-risk countries. We note that some overseas countries have introduced specific ECDD measures where high-risk countries are involved which could guide a New Zealand approach, including: • Obtaining additional information on the customer and on the beneficial owner • Obtaining additional information on the intended nature of the business relationship • Obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner(s) • Obtaining the approval of senior management for establishing or continuing the business relationship • Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transaction that need further examination
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?	

#	Question	Response
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?	
(4) Preventative measures – suspicious activity reporting		
4.203	How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?	We would welcome formal feedback from the FIU to reporting entities and supervisors on report quality. It would be useful to know what reports are valuable and what are not. We would also welcome FIU guidance: • differentiating the scenarios deemed reportable/non-reportable. • clarifying whether in-direct filing (meaning a reporting entity or its client are not the direct subject in the case) is deemed as defensive filing and not qualified as FIU reportable. • clarifying whether only the information owned by the reporting entity (e.g. client's information and transaction details processed by the reporting entity) should be included in the filing. We note that there are more FinTech businesses which leverage new transaction/routing models, which increases the instances where a reporting entity or its client is involved in part of the transaction. In these instances, the reporting entity might come across more details such as a client's underlying customer's details, additional information obtained by a counter-party bank during a reporting entity's investigation process, and information provided by a Police officer on a non-client. It would be helpful if guidance can be published on these matters.

#	Question	Response
4.204	What barriers might you have to providing high quality reporting to the FIU?	For the in-direct cases mentioned in 4.203 above, often reporting entities do not possess the full details nor can they verify them (e.g. it is possible that a reporting entity does not know if the client's underlying client identity is genuine in a scam case). This may result in a victim's account is being mentioned as a perpetrator because it was fraudulently opened by an unknown perpetrator. It would be helpful if more guidance can be shared by the FIU on this and whether a reporting entity should flag the case as "involved as an intermediary/third party" if this type of scenario is deemed reportable to FIU.
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?	In our view, the Act should allow for information sharing about SARs within a Group structure for the purpose of managing AML/CFT. Information pertaining to SARs should not be shared externally unless specifically permitted under law. The Act should therefore review the circumstances under which sharing of SAR-related information can be permitted.
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?	Yes. MVTS cross-border wire transfer money flow is often arranged into two domestic payments without a physical SWIFT message. In substance the transaction is a cross border payment but in definition it is still considered to be two domestic payments (1st domestic payment in NZ, and 2nd domestic payment in another country). Due to the current domestic payment processes, some details are not included nor validated (e.g. whether the beneficiary name is correctly presented as the beneficial account holder) within these payments, leading to a discount in transaction monitoring due to missing information and/or incorrect details presented on the domestic payments.
(5) Other issues or topics – privacy and protection of information		
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?	NZBA recommends full consultation with the Privacy Commissioner in agreeing retention periods, information sharing and other disclosure.
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?	
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?	

#	Question	Response
5.11	Is the process for testing assertions that a document or piece of information is privileged set out in section 159A appropriate?	
(5) Other issues or topics – 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?	It is important that the development of digital ID Service Trust Framework legislation and supporting rules are aligned with AML/CFT and Identity Verification requirements, and be capable of being relied on for the purposes of fulfilling these requirements. This will enable greater buy-in from the private sector and in turn should ensure that wider consumer benefits are realised. Private and public sector collaboration on this will be crucial. Striking the balance between ease of use and end user safety could be difficult. A further challenge could be the cost of implementing the solution without an understanding of how much it will be utilised; will it be viable/worth it?
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?	
(5) Other issues and topics – harmonisation with Australian regulation		
5.15	Should we achieve greater harmonisation with Australia's regulation? If so, why and how?	NZBA would welcome greater harmonisation of the New Zealand AML/CFT regime with Australia's regulation. Some of our members are multinational firms and operate in both Australia and New Zealand. Many of their customers in Australia are also customers in New Zealand, and many of their New Zealand customers based in New Zealand have a business relationship with Australian legal entities. There is a lot of overlap of people, systems and controls in Australia and New Zealand. Teams often cover both countries (including AML/CFT Compliance). The New Zealand regime could harmonise with Australia in these areas: • Introducing the concept of a 'Verifying Officer' to identify and verify persons acting on behalf of customers. • Including the Due Diligence by Customer Type into the Act/Rules. • Updating the Tipping Off and Correspondent Banking provisions. • Aligning record retention - 7 years (Australia) vs 5 years (New Zealand)
(6) Minor changes		
6.1	6.1 What are your views regarding the minor changes we have identified? Are there any that you do not support? Why?	SARs/PTRS

#	Question	Response
		<u>Issue</u>: The requirements set out in regulations for prescribed transaction reports made for international wire transfers are unclear about whether the country noted should be where the account is held or the country of the originator. *<u>Proposal for change</u>: Amend the regulation to obtain both the location of the account and the address of the sender to capture all relevant country information.* This is not likely to be 'minor' change from an implementation perspective as it will require material assessment for impact and compliance/automation for all payment types, for all New Zealand banks. It may also not be possible to have this as a mandatory obligation, depending on the payment information received. We recommend consultation with industry on any proposed change. If this proposal is implemented, which location is to be reported and/or used for reporting purposes; where the account is held or where the originator/sender is? If it is the sender, this may lead to PTRs not being reported as they may appear as domestic payments. <u>Preventative Measures</u> *<u>Issue</u>: There is no requirement that copies of records must be stored in New Zealand, particularly copies of customer identification documents.* *<u>Proposal for change</u>: Issue a regulation which requires businesses to retain copies of records in New Zealand to ensure they can be easily accessible when required.* We query whether this be required where scanned images are also held in secure digital format? For overseas banks with offshore based systems and procedures, the information is accessible to New Zealand based personnel where the information is also stored digitally.