Kokay, Nick

From: [redacted]@asb.co.nz>
Sent: Sunday, 12 December 2021 3:01 pm
To: [redacted]
Cc: [redacted]
Subject: Statutory Review - AML/CFT Act
Attachments: Statutory Review of the AMLCFT Act 2021 - ASB Response Final.docx

Categories: [redacted]

Be careful with this message!

This message contains one or more encrypted attachments that can't be scanned for viruses. Avoid downloading them unless you know the sender (verify the email address) and are confident that this email is legitimate.

Hi Nick

I hope all is well with you and that you're looking forward to a break over the holiday period.

As you'll be aware, ASB has been supporting the Statutory Review of the AML/CFT Act as a member of the banking sector. In November, we submitted our feedback on the consultation to the NZBA who are endeavouring to provide a consolidated response on behalf of their members next week. It's my understanding that the MOJ have received, and are continuing to receive feedback both directly from industry participants and as part of sector consultations. For completeness, kindly find attached ASB's feedback on the Statutory Review Consultation.

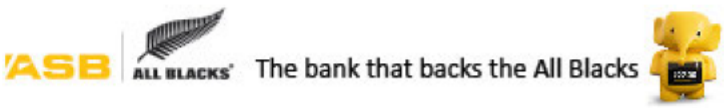
The P/W will follow by separate email.

If you have any questions, please do not hesitate to contact me.

Kindest regards
Mark

[redacted]
Head of Financial Crime Compliance | Compliance | Line 2 Risk | ASB
[redacted] | | [redacted]@asb.co.nz | **email**

Providing risk management guidance, review and challenge to keep our people and business safe



Review of the AML/CFT Act Part 1 - Institutional arrangements and stewardship	
Purpose of the AML/CFT Act	**ASB Response**
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?	ASB is of the view that the AML/CFT Act should have as its aim, the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. As such, we would support an expansion of the purpose to include 'prevention' as opposed to just focusing on deterrence or detection. However, the 'application' or operationalisation of this within the industry is important. ASB supports a clear and agreed-upon segregation of roles and responsibilities between Industry, Supervisory Authorities and Law Enforcement. It is not appropriate in all instances for a bank's internal processes to *confirm* or *verify* a link to money laundering or terrorist financing. Industry can only reach a *suspicion* – based on information available to it – which tells only part of the story. Law Enforcement has, at its disposal, broader information pertaining to the rest of the picture (e.g. communication, internet history, transactions involving other institutions etc.) and has within its remit the ability to charge perpetrators with offences. The onus should therefore be on law enforcement and if necessary, the courts to complete the transition from 'suspicion' to 'confirmed money laundering or terrorist financing'. Reporting Entities can provide intel upon request and can, theoretically, execute asset freezing upon direction so long as its provided for by law/regulation. Reporting Entities should not be forming views on whether or not funds are verifiably derived from illegal or illicit activities (or initiating action on that basis). If Reporting Entities are to engage in asset freezing, exiting, implementing account restrictions or preventing the use of accounts up-front, it's important that this be done pursuant to clear, defined and publicly acknowledged obligations. It cannot be solely driven by a bank's risk-based approach or internal risk appetite.
1.2 Should a purpose of the Act be that it seeks to actively prevent money laundering and terrorism financing, rather than simply deterring or detecting it?	
1.3. If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there need to be any additional or updated obligations for businesses?	
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?	ASB is supportive of expanding the purpose of the Act to include the countering of proliferation of weapons of mass destruction. Although, it does not make sense to specify particular regions or countries – would recommend that the purpose be linked to sanctions regime which will likely be updated in line with suspected activity in this space.
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?	
1.6. Should the Act support the implementation terrorism and proliferation financing targeted financial sanctions, required under the Terrorism Suppression Act 2002 and United Nations Act 1946? Why or why not?	
Risk-based approach to regulation	
1.7. What could be improved about New Zealand's framework for sharing information to manage risks?	ASB supports risk-based supervision in order to ensure that available resources are targeted towards those with the ability to have the greatest impact on financial stability, the consumer, or in an AML/CFT context, where the risk of ML/TF is greatest.

	A potential suggestion is the use of something akin to the PRISM model (Probably Risk and Impact SysteM™) used in Ireland. Used as a tool to support risk-based supervision, it explicitly recognises that we can only have a finite number of supervisors and that we must deploy them where they can make the greatest difference. While it is used across all forms of supervision (including prudential and conduct), the premise is that one establishes a means and methodology to risk-assess the firms under supervision, and then agrees the frequency and intensity of supervision as warranted by the documented risks. Information can be found on PRISM™ here: https://www.centralbank.ie/regulation/how-we-regulate/supervision/prism With regard to information sharing, ASB is of the view that there must be a clear lawful basis for the disclosure of customer information. Feedback summarised below: 1. With regard to customer risk, if the intention is for customer-related information to be shared within the industry (i.e. and not just with supervisory authorities or law enforcement bodies) for the purposes of risk management, then a section within the Act expressly permitting this, and the conditions under which it would be permitted, would be welcomed. Such a move should involve direct engagement with the Privacy Commissioner. 2. In addition, the obligations on Reporting Entities with regard to subsequent action off the back of customer information obtained would need clarification. For example, if information pertaining to a SAR reported by another bank is obtained by ASB, is ASB under an obligation to report/exit/heighten the risk rating of the customer? 3. Once the CDD Programmes of reporting entities become sufficiently mature, and the respective back-books are refreshed to a significant degree, there is an opportunity for the Act to allow reliance on the fact that the customer's identity has been verified to the same standard externally.
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?	No comments from ASB on Section 58 in terms of requirements. Consideration might be given to produce best practice examples of risk assessment formats across low, medium and high impact reporting entities.
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?	ASB is supportive of retaining the risk-based approach contained within the legislation (i.e. risk-based and principle-driven) but with additional clarity on expectations through guidance, codes of practice etc. There are opportunities 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 ML/TF' – thereby putting the onus on the reporting entity to assess the risk involved and act accordingly. The entity can then be challenged by the supervisor on whether or not the risks have been appropriately considered and assessed, and whether or not the actions are adequate.

	Prescriptive or explicit requirements under the Act should be reserved for instances where risk-based approach is not appropriate or where all reporting entities should have the same position on the risk involved. As an example, Trusts carry varying degrees of risk depending on their structure, set-up, complexity etc. Having ECDD apply in all instances is not risk-based – it carries an administrative burden disproportionate to risk involved in certain circumstances and doesn't allow the reporting entities to apply the CDD measures as warranted by the risk of ML/TF. Conversely, there are opportunities to introduce prescriptive requirements which align with the risks involved. For example, we could consider the following: - Expressly prohibiting the application of simplified CDD where there is a suspicion of money laundering or terrorist financing or where a SAR has been raised - Specific trigger events which should result in the application of OCDD e g. o Where a customer takes out a new product o Explicit requirement in the AML/CFT Act that CDD be conducted where there are doubts about the veracity or adequacy of previously obtained data o Where there is a suspicion of ML/TF - This could take the form of baseline de minimis obligations which could then be added to by reporting entities as warranted by the risks involved.
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?	ASB supports an Act which sets out risk-based principles and obligations which is then supplemented and supported through the use of guidance material, codes of practice etc. Suggestions include: - Examples of Risk Assessments performed in low, moderate and high-rated businesses - Suggested (or even mandated) Ongoing Customer Due Diligence Triggers - SOF/SOW
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?	
1.14. Are exemptions still required for the regime to operate effectively? If not, how can we ensure AML/CFT obligations are appropriate for low-risk businesses or activities?	
1.15. Is the Minister of Justice the appropriate decision maker for exemptions under section 157, or should it be an operational decision maker such as the Secretary of Justice? Why or why not?	
1.16. Are the factors set out in section 157(3) appropriate?	
1.17. Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?	
1.18. Should the Act specify what applicants for exemptions under section 157 should provide? Should there be a simplified process when applying to renew an existing exemption?	
1.19. Should there be other avenues beyond judicial review for applicants if the Minister decides not to grant an exemption? If so, what could these avenues look like?	
1.20. Are there any other improvements that we could make to the exemptions function? For example, should the process be more formalised with a linear documentary application process?	
Mitigating unintended consequences	
1.21. Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?	

1.22. How could the regime better protect the need for people to access banking services to properly participate in society?	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 & monitor or exit & prevent. A potential suggestion is allowing a defined basic banking service to be available to all customers, exempt from an obligation to de-bank or exit (but 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 relationship.
1.23. Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them?	Unintended consequences of de-risking/de-banking include: (a) The removal or deterioration of services for members of the Pacific Island community. ASB recommends that MSBs be brought fully under the AML/CFT legislative regime, and the introduction of specific MSB due diligence and ongoing MSB due diligence obligations in order to allow those who engage with them to rely on the AML/CFT Programme held by the MSB – subject to the due diligence and ongoing monitoring undertaken. It is also recommended that the concept of POWBATIC is removed.
The role of the private sector	
1.24. Can the Act do more to enable private sector collaboration and coordination, and if so, what?	ASB supports the concept of private sector collaboration and coordination in principle, particularly insofar as it pertains to policy issues which have the potential to assist NZ Inc. However, the sharing of information between private and public sector, and within the private sector carries privacy and anti-competitive practice implications which need to be considered fully. It is very important that the Act sets out what is permitted, under what circumstances and for what explicit lawful purpose. For example, should exits be permitted upon receipt of SAR-related 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 relationship? A suggestion is adopting an 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 an NDA. A further example is the Digital ID Trust Framework Initiative – particularly in the context of E-IDV. NEMID (Danish E-IDV) can be used for most public sector orgs and banks etc. and was the result of collaboration between banks and supervisory authorities/government. With regard to regulatory engagement, ASB supports the continued engagement levels that it has with its supervisor.
1.25. What do you see as the ideal future for public and private sector cooperation? Are there any barriers that prevent that future from being realised and if so, what are they?	
1.26. Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime?	
1.27. Should the Act require have a mechanism to enable feedback about the operation and performance of the Act on an ongoing basis? If so, what is the mechanism and how could it work?	
Powers and functions of AML/CFT agencies	
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?	ASB supports, in principle, the FIU being able to request information from businesses as required to discharge their obligations and support investigations. However, it's important that the necessary consultation happens between FIU and Industry so that agreeable SLAs can be established, and privacy risks are appropriately mitigated. The Act must cover (very clearly) the circumstances under which:
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?	(a) Information can be requested by the FIU (b) The timelines within which reporting entities must facilitate the requests (c) What information can be provided Any requests for information outside what should be explicit and prescriptive sets of circumstances within the Act should not be accommodated. ASB would expect full consultation on this to be carried out with the Privacy Commissioner. With regard to freezing, Again, ASB supports this power in principle – but only where explicitly prescribed for under the Act and with full clarity and transparency. In the event that asset freezing powers were used by the FIU, and Reporting Entities are directed to do so, REs must be allowed to notify the impacted customer – much in the same way that Sanctions-related asset freezing can be disclosed. Once asset freezing is activated, reporting entities cannot to continue to service customers without being able to explain why access to funds is being denied. As such, it is preferable that asset freezing should not be activated until the risk of tipping off is no longer a factor. If tipping off is to remain a factor, reporting entities must be fully protected by the Act in the event that legal action is pursued by the customer whose assets have been frozen. Consideration should also be given to the impact of asset freezing on lending products or day-to-day transactional accounts. The reputational impact to banks in the event that cards used for basic day-to-day needs or meeting mortgage payments were frozen would be significant.
1.31. If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?	
1.32. Should the Act provide the FIU with a power to freeze, on a time limited basis, funds or transactions in order to prevent harm and victimisation? If so, how could the power work and operate? In what circumstances could the power be used, and how could we ensure it is a proportionate and reasonable power?	
1.33. How can we avoid potentially tipping off suspected criminals when the power is used?	
1.34. Should supervision of implementation of TFS fall within the scope of the AML/CFT regime? Why or why not?	
1.35. Which agency or agencies should be empowered to supervise, monitor, and enforce compliance with obligations to implement TFS? Why?	
Secondary legislation making powers	
1.36. Are the secondary legislation making powers in the Act appropriate, or are there other aspects of the regime that could benefit from having regulation making powers created?	ASB does not support bestowing the authority on FIU to issue Codes of Practice. That authority should remain within regulation and therefore with the supervisory authorities in order to appropriately segregate regulation and law enforcement and mitigate the risk of inconsistent interpretation. ASB supports the use of Codes of Practice. However, it's important that they are consistently interpreted across the three supervisory authorities in their application. ASB would recommend additional use of case studies and examples of good and bad practice – particularly with respect to: - Ongoing Customer Due Diligence (triggers) - SOF/SOW - Risk Assessment Methodologies - Training - Monitoring & Assurance (including system assurance)
1.37. How could we better use secondary legislation making powers to ensure the regime is agile and responsive?	
1.38. Are the three Ministers responsible for issuing Codes of Practice the appropriate decision makers, or should it be an operational decision maker such as the chief executives of the AML/CFT supervisors? Why or why not?	
1.39. Should the New Zealand Police also be able to issue Codes of Practice for some types of FIU issued guidance? If so, what should the process be?	
1.40. Are Codes of Practice a useful tool for businesses? If so, are there any additional topics that Codes of Practice should focus on? What enhancements could be made to Codes of Practice?	
1.41. Does the requirement for businesses to demonstrate they are complying through some equally effective means impact the ability for businesses to opt out of a Code of Practice?	
1.42. What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool?	
1.43. Should operational decision makers within agencies be responsible for making or amending the format of reports and forms required by the Act? Why or why not?	

1.44. If so, which operational decision makers would be appropriate, and what could be the process for making the decision? For example, should the decision maker be required to consult with affected parties, and could the formats be modified for specific sectoral needs?	
1.45. Would AML/CFT Rules (or similar) that prescribed how businesses should comply with obligations be a useful tool for business? Why or why not?	
1.46. If we allowed for AML/CFT Rules to be issued, what would they be used for, and who should be responsible for issuing them?	
Information sharing	
1.47. Would you support regulations being issued for a tightly constrained direct data access arrangement which enables specific government agencies to query intelligence the FIU holds? Why or why not?	No comments on this section.
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?	
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?	ASB supports risk-based supervision in order to ensure that available resources are targeted towards those with the ability to have the greatest impact on financial stability, the consumer, or in an AML/CFT context, where the risk of ML/TF is greatest. A suggestion is the use of something akin to the PRISM model (Probably Risk and Impact SysteM™) used in Ireland. Used as a tool to support risk-based supervision, it explicitly recognises that we can only have a finite number of supervisors and that we must deploy them where they can make the greatest difference. While it is used across all forms of supervision (including prudential and conduct), the premise is that one establishes a means and methodology to risk-assess the firms under supervision, and then agrees the frequency and intensity of supervision as warranted by the documented risks. Information can be found on PRISM™ here: https://www.centralbank.ie/regulation/how-we-regulate/supervision/prism
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?	
1.55. Should there also be an AML/CFT licensing regime in addition to a registration regime? Why or why not?	
1.56. If we established an AML/CFT licensing regime, how should it operate? How could we ensure the costs involved are not disproportionate?	
1.57. Should a regime only apply to sectors which have been identified as being highly vulnerable to money laundering and terrorism financing, but are not already required to be licensed?	
1.58. If such a regime was established, what is the best way for it to navigate existing licensing requirements?	
1.59. Would requiring risky businesses to be licensed impact the willingness of other businesses to have them as customers? Can you think of any potential negative flow-on effects	

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?	
Part 2 - Scope of the AML/CFT Act	
Challenges with existing terminology	
2.1. How should the Act determine whether an activity is captured, particularly for DNFBPs? Does the Act need to prescribe how businesses should determine when something is in the "ordinary course of business"?	No comments on this.
2.2. If "ordinary course of business" was amended to provide greater clarity, particularly for DFNBPs, how should it be articulated?	
2.3. Should "ordinary" be removed, and if so, how could we provide some regulatory relief for businesses which provide activities infrequently? Are there unintended consequences that may result?	
2.4. Should businesses be required to apply AML/CFT measures in respect of captured activities, irrespective of whether the business is a financial institution or a DNFBP? Why or why not?	
2.5. If so, should we remove "only to the extent" from section 6(4)? Would anything else need to change, e.g. to ensure the application of the Act is not inadvertently expanded?	
2.6. Should we issue regulations to clarify that captured activities attract AML/CFT obligations irrespective of the type of reporting entity which provides those activities? Why or why not?	
2.7. Should we remove the overlap between "managing client funds" and other financial institution activities? If so, how could we best do this to avoid any obligations being duplicated for the same activity?	
2.8. Should we clarify what is meant by 'professional fees'? If so, what would be an appropriate definition?	
2.9. Should the fees of a third party be included within the scope of 'professional fees'? Why or why not?	
2.10. Does the current definition appropriately capture those businesses which are involved with a particular activity, including the operation and management of legal persons and arrangements? Why or why not? How could it be improved?	
2.11. Have you faced any challenges with interpreting the activity of "engaging in or giving instructions"? What are those challenges and how could we address them?	
2.12. Should the terminology in the definition of financial institution be better aligned with the meaning of financial service provided in section 5 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008? If so, how could we achieve this?	
2.13. Are there other elements of the definition of financial institution that cause uncertainty and confusion about the Act's operation?	

2.14. Should the definition of high-value dealer be amended so businesses which deal in high value articles are high-value dealers irrespective of how frequently they undertake relevant cash transactions? Why or why not? Can you think of any unintended consequences that might occur?	
2.15. What do you anticipate would be the compliance impact of this change?	
2.16. Should we revoke the exclusion for pawnbrokers to ensure they can manage their money laundering and terrorism financing risks? Why or why not?	
2.17. Given there is an existing regime for pawnbrokers, what obligations should we avoid duplicating to avoid unnecessary compliance costs?	
2.18. Should we lower the applicable threshold for high value dealers to enable better intelligence about cash transactions? Why or why not?	
2.19. If so, what would be the appropriate threshold? How many additional transactions would be captured? Would you stop using or accepting cash for these transactions to avoid AML/CFT obligations?	
2.20. Do you currently engage in any transactions involving stores of value that are not portable devices (e.g. digital stored value instruments)? What is the nature and value of those transactions?	
2.21. What risks do you see with stored value instruments that do not use portable devices?	
2.22. Should we amend the definition of "stored value instruments" to be neutral as to the technology involved? If so, how should we change the definition?	
Potential new activities	
2.23. Should acting as a secretary of a company, partner in a partnership, or equivalent position in other legal persons and arrangements attract AML/CFT obligations?	No comments on this.
2.24. If you are a business which provides this type of activity, what do you estimate the potential compliance costs would be for your business if it attracted AML/CFT obligations? How many companies or partnerships do you provide these services for?	
2.25. Should criminal defence lawyers have AML/CFT obligations? If so, what should those obligations be and why?	
2.26. If you are a criminal defence lawyer, have you noticed any potentially suspicious activities? Without breaching legal privilege, what were those activities and what did you do about them?	
2.27. Are there any unintended consequences that may arise from requiring criminal defence lawyers to have limited AML/CFT obligations, that we will need to be aware of?	
2.28. Should non-life insurance companies become reporting entities under the Act?	
2.29. If so, should non-life insurance companies have full obligations, or should they be tailored to the specific risks we have identified?	
2.30. If you are a non-life insurance business, what do you estimate would be the costs of having AML/CFT obligations (including limited obligations)?	
2.31. Should we use regulations to ensure that all types of virtual asset service providers have AML/CFT obligations, including by declaring wallet providers which only provide safekeeping or administration are reporting entities? If so, how should we?	
2.32. Would issuing regulations for this purpose change the scope of capture for virtual asset service providers which are currently captured by the AML/CFT regime?	
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?	
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?	No comments on this
2.40. Should the exemption for internet auctions still apply, and are the settings correct in terms of a wholesale exclusion of all activities?	
2.41. If it should continue to apply, should online marketplaces be within scope of the exemption?	
2.42. What risks do you see involving internet marketplaces or internet auctions?	
2.43. If we were to no longer exclude online marketplaces or internet auction providers from the Act, what should the scope of their obligations be? What would be the cost and impact of that change?	
2.44. Do you currently rely on this regulatory exemption to offer special remittance card facilities? If so, how many facilities do you offer to how many customers?	
2.45. Is the exemption workable or are changes needed to improve its operation? What would be the impact on compliance costs from those changes?	
2.46. Do you consider the exemption properly mitigates any risks of money laundering or terrorism financing through its conditions?	
2.47. Should we amend this regulatory exemption to clarify whether and how it applies to DNFBPs? If so, how?	
Potential new regulatory exemptions	
2.48. Should we issue any new regulatory exemptions? Are there any areas where Ministerial exemptions have been granted where a regulatory exemption should be issued instead?	No comments on this
2.49. Do you currently use a company to provide trustee or nominee services? If so, why do you use them, and how many do you use? What is the ownership and control structure for those companies?	
2.50. Should we issue a new regulatory exemption to exempt legal or natural persons that act as trustee, nominee director, or nominee shareholder where there is a parent reporting entity involved that is responsible for discharging their AML/CFT obligations? Why or why not?	
2.51. If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?	
2.52. Should we issue a new regulatory exemption to exempt Crown entities, entities acting as agents of the Crown, community trusts, and any other similar entities from AML/CFT obligations?	
2.53. If so, what should be the scope of the exemption and possible conditions to ensure it does not raise other money laundering or terrorism financing vulnerabilities?	
2.54. Should we issue an exemption for all reporting entities providing low value loans, particularly where those loans are provided for social or charitable purposes?	
2.55. If so, what conditions should be attached to such an exemption to ensure it does not raise other money laundering or terrorism financing vulnerabilities?	
Territorial scope	
2.56. Should the AML/CFT Act define its territorial scope?	No comments on this
2.57. If so, how should the Act define a business or activity to be within the Act's territorial scope?	
Part 3 - Supervision, regulation, and enforcement	

Agency supervision model	
3.1. Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it?	ASB supports risk-based supervision in order to ensure that available resources are targeted towards those with the ability to have the greatest impact on financial stability, the consumer, or in an AML/CFT context, where the risk of ML/TF is greatest. A suggestion is the use of something akin to the PRISM model (Probably Risk and Impact SysteM™) used in Ireland. Used as a tool to support risk-based supervision, it explicitly recognises that we can only have a finite number of supervisors and that we must deploy them where they can make the greatest difference. While it is used across all forms of supervision (including prudential and conduct), the premise is that one establishes a means and methodology to risk-assess the firms under supervision, and then agrees the frequency and intensity of supervision as warranted by the documented risks. Information can be found on PRISM™ here: https://www.centralbank.ie/regulation/how-we-regulate/supervision/prism ASB also fully supports consistency in the application of the Act. A potential suggestion is the potential amalgamation of the three supervisors for the purposes of AML/CFT supervision.
3.2. If it were to change, what supervisory model do you think would be more effective in a New Zealand context?	
3.3. Do you think the Act appropriately ensures consistency in the application of the law between the three supervisors? If not, how could inconsistencies in the application of obligations be minimised?	
3.4. Does the Act achieve the appropriate balance between ensuring consistency and allowing supervisors to be responsive to sectoral needs? If not, what mechanisms could be included in legislation to achieve a more appropriate balance?	
Powers and functions	
3.5. Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why?	ASB supports the introduction of a digital or electronic form (current option is limited to paper-based). Furthermore, 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 assess via audits and onsite visits.
3.6. Should AML/CFT Supervisors have the power to conduct onsite inspections of REs operating from a dwelling house? If so, what controls should be implemented to protect the rights of the occupants?	
3.7. What are some advantages or disadvantages of remote onsite inspections?	
3.8. Would virtual inspection options make supervision more efficient? What mechanisms would be required to make virtual inspections work?	
3.9. Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient?	
3.10. Should supervisors have an explicit role in approving or rejecting formation of a DBG? Why or why not?	
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?	No comments on this
3.12. Who would be responsible for enforcing the standards of auditors?	
3.13. What impact would that have on cost for audits? What benefits would there be for businesses if we ensured higher quality audits?	
3.14. Should there be any protections for businesses which rely on audits, or liability for auditors who do not provide a satisfactory audit?	
3.15. Is it appropriate to specify the role of a consultant in legislation, including what obligations they should have? If so, what are appropriate obligations for consultants?	
3.16. Do we need to specify what standards consultants should be held to? If so, what would it look like? Would it include specific standards that must be met before providing advice?	
3.17. Who would be responsible enforcing the standard of consultants?	
3.18. Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for?	

3.19. Do you currently take any steps to ensure that only appropriate persons are able to act as your agent? What are those steps and why do you take them?	
3.20. Should there be any additional measures in place to regulate the use of agents and third parties? For example, should we set out who can be an agent and in what circumstances they can be relied upon?	
Offences and penalties	
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?	ASB supports a penalty framework which is fair, transparent, risk-based and which dissuades non-compliance and rewards positive behaviour. A potential suggestion is the introduction of a penalty framework which sets out the relevant factors and thresholds contributing to fines and penalties (customer impact, length of time gap was in place, materiality), and indeed the actions which can reduce exposure (e.g. proactive engagement, self-identified etc.) As customer or transaction-based requirements are in place for growing timeframes (e.g. CDD and PTR), the relative impact of breaches in transactional terms is only going to grow – therefore, it's important that breaches are assessed using factors other than just 'how many accounts were involved'. It's important that risk functions are able to assess regulatory risk exposure as accurately and clearly as possible for their Boards.
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?	
3.25. Would broadening the scope of civil sanctions to include directors and senior management support compliance outcomes? Should this include other employees?	
3.26. If penalties could apply to senior managers and directors, what is the appropriate penalty amount?	
3.27. Should compliance officers also be subject to sanctions or provided protection from sanctions when acting in good faith?	
3.28. Should DIA have the power to apply to liquidate a business to recover penalties and costs obtained in proceedings undertaken under the Act?	
3.29. Should we change the time limit by which prosecutions must be brought by? If so, what should we change the time limit to?	
Part 4 - Preventive measures	
Customer due diligence	
4.1. What challenges do you have with complying with your CDD obligations? How could these challenges be resolved?	ASB recommends the following with respect to Customer Due Diligence - **Removal of Address Verification:** While address verification is useful in contributing to the assessment of jurisdictional risk and the prevention of fraud, the current obligations are not fit for purpose and cause a disproportionate impact on customers. It's recommended that the obligation to obtain address verification be removed from the customer due diligence section of the Act in all circumstances (including high-risk customers). A potential replacement could be the obligation to obtain and validate mobile phone number or email address. - **ECDD on Trusts:** There are different types of trusts each with varying degree of risk exposure from a money laundering or terrorist financing perspective. As such, the obligation to apply ECDD on Trusts should be amended to incorporate that nuance. Entities should be able to risk-rate Trusts based on the difference types, and apply CDD measures according to the levels of risk involved.
4.2. Have you experienced any situations where trying to identify the customer can be challenging or not straightforward? What were those situations and why was it challenging?	
4.3. Would a more prescriptive approach to the definition of a customer be helpful? For example, should we issue regulations to define who the customer is in various circumstances and when various services are provided?	
4.4. If so, what are the situations where more prescription is required to define the customer?	
4.5. Do you anticipate that there would be any benefits or additional challenges from a more prescriptive approach being taken?	
4.6. Should we amend the existing regulations to require real estate agents to conduct CDD on both the purchaser and vendor?	
4.7. What challenges do you anticipate would occur if this was required? How might these be addressed? What do you estimate would be the costs of the change?	
4.8. When is the appropriate time for CDD on the vendor and purchaser to be conducted in real estate transactions?	
4.9. Are the prescribed points where CDD must be conducted clear and appropriate? If not, how could we improve them?	
4.10. For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear?	

4.11. Should CDD be required in all instances where suspicions arise?	- **Beneficial Ownership:** It is recommended that consideration to beneficial ownership more holistically be given – in line with EU's Beneficial Ownership regime with the following changes recommended: o Establish a central public Beneficial Ownership Register (for Entities) and a Trust Register o Require all companies to create their own individual Beneficial Ownership Registers and to keep the public register updated as details change o Define beneficial ownership for the purposes of all entity types within the legislation itself o Require that verification of beneficial ownership extends only so far as warranted by the risk of ML/TF. The more complex the arrangement (or heightened the risk), the more verification is required o Establish a Trust register and require Trustees to create beneficial ownership registers for each trust and keep the public register up-to-date. o Include specific obligations on what it required vis-à-vis beneficial ownership verification on an ongoing basis This should help bring clarity to obligations and a more readily available source to use when discharging the obligations.
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?	
4.14. What money laundering risks are you seeing in relation to law firm trust accounts?	
4.15. Are there any specific AML/CFT requirements or controls that could be put in place to mitigate the risks? If so, what types of circumstances or transactions should they apply to and what should the AML/CFT requirements be?	
4.16. Should this only apply to law firm trust accounts or to any DNFBP that holds funds in its trust account?	
4.17. What do you estimate would be the costs of any additional controls you have identified?	
4.18. Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?	
4.19. Are the obligations to obtain and verify information clear?	
4.20. Is the information that businesses should obtain and verify about their customers still appropriate?	
4.21. Is there any other information that the Act should require businesses to obtain or verify as part of CDD to better identify and manage a customer's risks?	
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?	- **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.
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?	- **Remove 'wet ink' Certification Requirements:** It is recommended that the obligation to obtain 'wet ink' certification on ID documents be remove. It doesn't add value.
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?	- **Simplified CDD:** Prohibit the use of simplified CDD measures where there is a risk of money laundering or terrorist financing
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?	- **Reliance & 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.
4.26. Are there any instances where businesses should not be required to obtain this information? Are there any circumstances when source of funds and source of wealth should be obtained and verified?	
4.27. Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds?	- **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 performing by the intermediary who holds the relationship with the underlying customer.
4.28. Should we issue regulations to require businesses to obtain information about the beneficiary/ies of a life insurance or investment-related insurance policy and prescribe the beneficiary/ies as a relevant risk factor when determining the appropriate level of CDD to conduct? Why or why not?	
4.29. If we required this approach to be taken regarding beneficiaries of life and other investment-related insurance policies, should the obligations only apply for moderate or high-risk insurance policies? Are there any other steps we could take to ensure compliance costs are proportionate to risks?	- **MSB Due Diligence:** Introduce prescribed due diligence requirements on MSBs (inline with requirements which current apply to correspondent banking relationships)
4.30. Have you encountered issues with the definition of a beneficial owner? If so, what about the definition was unclear or problematic?	- **RMA Due Diligence:** Confirm whether any due diligence obligations should extend to RMAs and the circumstances under which they should
4.31. How can we improve the definition in the Act as well as in guidance to address those challenges?	

Commented [KN1]: Relationship Management Applications – it's a term used in the context of correspondent banking arrangements. RMA-only relationships between banks involve the exchange of authenticated Swift messages but don't involve Vostro accounts, credit or banking facilities – and are therefore lower risk from an ML/TF perspective. The RBNZ has previously advised by way of guidance that the due diligence requirements set out in Section 29 of the Act do not apply to RMA-only relationships.

The question we've posed in our response to the consultation is whether or not any form of due diligence should be applied to RMA-only relationships, and should the need (or lack thereof) to apply measures to RMAs be detailed in the Act.

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?	- **Tipping Off:** Introduce a line in the Act which allows for reporting entities to not perform CDD where there is a risk of tipping off. Have this at the discretion of the reporting entity but allow for this to be challenged via assurance, audits, onsite visits etc. - **CDD**: Introduce explicit requirements to perform CDD where: o There is a doubt to the adequacy or veracity of CDD on file o There is a suspicions of money laundering or terrorist financing - **Additional Guidance:** It is recommended that additional guidance be provided on CDD with regards to the following circumstances: o Minors o Vulnerable situations (care homes, homeless etc.) - **Expired ID Documents:** Would welcome formal position on the use of expired documentation in verifying identity. - **Electronic ID Verification:** ASB recommends 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 in this space. The Digital Identity Services Trust Framework Bill aims to promote the provision of secure digital identity services 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 laws have, as a baseline, alignment with AML/CTF 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. - o In order to more easily meet the requirements of section 15e) of the Part 3 of the AML-CFT-identity-verification-code-of-practice-2013 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. o 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 (particular 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 17e) (linking the customer to the claimed identity). We request that consideration be given to: ▪ Removal of the requirement in 15a) for two independent and reliable matching electronic sources OR
4.33. To extent are you focusing beneficial ownership checks on the 'ultimate' beneficial owner, even though it is not strictly required?	
4.34. Would there be any additional costs resulting from prescribing that businesses should focus on the 'ultimate' beneficial owner?	
4.35. Should we issue a regulation which states that for the purposes of the definition of beneficial owner, a person on whose behalf a transaction is conducted is restricted to a person with indirect ownership or control of the customer (to align with the FATF standards)? Why or why not?	
4.36. Would this change make the "specified managing intermediaries" exemption or Regulation 24 of the AML/CFT (Exemption) Regulations 2011 unnecessary? If so, should the exemptions be revoked?	
4.37. Would there be any additional compliance costs or other consequences for your business from this change? If so, what steps could be taken to minimise 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?	
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?	
4.43. Would there be an impact on your compliance costs by mandating that this process be applied? If so, what is the impact?	
4.44. Should we remove the requirement for enhanced CDD to be conducted for all trusts or vehicles for holding personal assets? Why or why not?	
4.45. 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?	
4.46. 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?	
4.47. Are the standards of verification and the basis by which verification of identity must be done clear and still appropriate? If not, how could they be improved?	
4.48. What challenges have you faced with verification of address information? What have been the impacts of those challenges?	
4.49. In your view, when should address information be verified, and should that verification occur?	
4.50. 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?	
4.51. Do you currently take any of the steps identified by the FATF standards to manage high-risk customers, transactions or activities? If so, what steps do you take and why?	
4.52. Should we issue regulations or a Code of Practice which outlines the additional measures that businesses can take as part of enhanced CDD?	
4.53. Should any of the additional measures be mandatory? If so, how should they be mandated, and in what circumstances?	

4.54. Are there ways we can enhance or streamline the operation of the simplified CDD obligations, in particular where the customer is a large organisation?	▪ Further clarity on whether the expectation for "matching" requires a perfect / identical match or whether there is some tolerance 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 measures could be available under safe harbour to confirm a secondary existence of the customer's identity without specifically the name needing to match across two electronic sources. - **Information Sharing**: Recommend consideration be given to the advantages of those departments sharing information with reporting entities to support us to conduct compliant CDD and reduce identity theft. Examples include: o NZTA supplying a photo when confirming identity matches o And possibly DIA/Immigration enabling the querying of immigration data for non-NZers.
4.55. Should we issue regulations to allow employees to be delegated by a senior manager without triggering CDD in each circumstance? Why?	
4.56. Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?	
4.57. As part of ongoing CDD and account monitoring, do you consider whether and when CDD was last conducted and the adequacy of the information previously obtained?	
4.58. Should we issue regulations to require businesses to consider these factors when conducting ongoing CDD and account monitoring? Why?	
4.59. What would be the impact on your compliance costs if we issued regulations to make this change? Would ongoing CDD be triggered more often?	
4.60. Should we mandate any other requirements for ongoing CDD, e.g. frequently it needs to be conducted?	
4.61. If you are a DNFBP, how do you currently approach your ongoing CDD and account monitoring obligations where there are few or no financial transactions?	
4.62. Should we issue regulations to require businesses to review activities provided to the customer as well as account activity and transaction behaviour? What reviews would you consider to be appropriate?	
4.63. What would be the impact on your compliance costs if we issued regulations to make this change?	
4.64. Do you currently review other information beyond what is required in the Act as part of account monitoring? If so, what information do you review and why?	
4.65. 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?	
4.66. 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?	
4.67. Should the Act set out what can constitute tipping off and set out a test for businesses to apply to determine whether conducting CDD or enhanced CDD may tip off a customer?	
4.68. Once suspicion has been formed, should reporting entities have the discretion not to conduct enhanced CDD to avoid tipping off?	
4.69. 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)?	
4.70. Are there any other challenges with the existing requirements to conduct enhanced CDD as soon as practicable after becoming aware that a SAR must be reported? How could we address those challenges?	
Record keeping	
4.71. Do you have any challenges with complying with your record keeping obligations? How could we address those challenges?	ASB supports clarity in the record-keeping space, If specified retention periods are to be included, it's important that these be reconciled with retention obligations that may exist in other spaces. For example, many firms retain records for longer than retention periods in order to protect themselves against future allegations of misconduct or fraud. If retention periods are to be included, we must
4.72. Are there any other records we should require businesses to keep, depending on the nature of their business?	

4.73. 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?	ensure that there is a statute of limitations on allegations of misconduct so that reporting entities aren't left with a compromised defence of their conduct.
Politically exposed persons	
4.74. Do you have any challenges with complying with the obligations regarding politically exposed persons? How could we address those challenges?	ASB supports the following with respect to Politically Exposed Persons: - **Extension to Include Domestic**: From a risk-based perspective, there is no difference between foreign and domestic PEPs. A PEPs susceptibility to risks of bribery, corruption or other predicate offences is not heightened by being 'foreign'. As such, at a principle level, ASB would support the inclusion of domestic PEPs in the definition under the ACT. - **Clarity on Associated Persons**: Extending the definition to include domestic PEPs will, in a relatively small country have some unintended consequences given the likely connectivity between NZers. On that basis, its recommended that the concept of related or associated persons be more narrowly defined and be allowed on a risk-based basis. - **Centralised List of Prominent Public Functions**: Other regions globally have commenced creating a list of prominent public functions for the purposes of ensuring that ECDD measures on PEPs are only applied in intended instances. This is recommended for NZ.
4.75. Do you take any additional steps to mitigate the risks of PEPs that are not required by the Act? What are those steps and why do you take them?	
4.76. How do you currently treat customers who are domestic PEPs or PEPs from international organisations?	
4.77. Should the definition of 'politically exposed persons' be expanded to include domestic PEPs and/or PEPs from international organisations? If so, what should the definitions be?	
4.78. 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?	
4.79. What would be the cost implications of such a measure for your business or sector?	
4.80. How do you currently treat customers who were once PEPs?	
4.81. 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?	
4.82. Would a risk-based approach to former PEPs impact compliance costs compared to the current prescriptive approach?	
4.83. What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP?	
4.84. 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?	
4.85. Should the Act clearly allow business to consider their level of exposure to foreign PEPs when determining the extent to which they need to take proactive steps?	
4.86. 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?	
4.87. How do you currently deal with domestic PEPs or international organisation PEPs? For example, do you take risk-based measures to determine whether a customer is a domestic PEP, even though our law does not require this to be done?	
4.88. 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?	
4.89. What would the cost implications of including domestic PEPs and PEPs from international organisations be for your business or sector?	
4.90. 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?	
4.91. What would be the cost implications of requiring life insurers to determine whether a beneficiary is a PEP?	
4.92. What steps do you currently take to mitigate the risks of customers who are PEPs?	
4.93. Should the Act mandate businesses take the necessary mitigation steps the FATF expects for all foreign PEPs, and, if domestic or international organisation PEPs are included within scope, where they present higher risks?	

4.94. What would be the cost implications of requiring businesses to take further steps to mitigate the risks of customers who are PEPs?	
Implementation of targeted financial sanctions	
4.95. Should businesses be required to assess their exposure to designated individuals or entities?	ASB supports the inclusion of targeted financial sanctions within a reporting entity's overall Compliance Programme with the following feedback: - The sanctions programme should be able to be standalone (it should need to be part of the AML/CFT Programme) - However, the sanctions programme requirements should be defined so that they can be assessed accordingly and subject to a consistent level of regulatory scrutiny by the supervisory authorities - Recommend the introduction of a sanction risk assessment – with specific guidance on what to include - Recommend the introduction of a requirement to assess the sanctions risks associated with products, channels and technologies. - Consideration could be given to having the supervisors collate and centralise the list-based screening required to be performed by reporting entities - Recommend having one supervisor responsible for oversight of sanctions compliance to ensure consistent interpretation of obligations and enforcement of same
4.96. What support would businesses need to conduct this assessment?	
4.97. 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?	
4.98. Should legislation require businesses to include, as part of their AML/CFT programme, policies, procedures, and controls to implement TFS obligations without delay? How prescriptive should the requirement be?	
4.99. What support would businesses need to develop such policies, procedures, and controls?	
4.100. How should businesses receive timely updates to sanctions lists?	
4.101. 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?	
4.102. How can we support and enable businesses to identify associates and persons acting on behalf of designated persons or entities?	
4.103. Do you currently screen for customers and transactions involving designated persons and entities? If so, what is the process that you follow?	
4.104. 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?	
4.105. If we created obligations in the Act, how could we ensure that the obligations can be implemented efficiently and that we minimise compliance costs?	
4.106. How can we streamline current reporting obligations and ensure there is an appropriate notification process for property frozen in compliance with regulations issued under the United Nations Act?	
4.107. If we included a new reporting obligation in the Act which complies with UN and FATF requirements, how could that obligation look? How could we ensure there is no duplication of reporting requirements?	
4.108. Should the government provide assurance to businesses that have frozen assets that the actions taken are appropriate?	
4.109. If so, what could that assurance look like and how would it work?	
Correspondent banking	
4.110. 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?	Nothing in addition to feedback outlined in CDD.
4.111. Are you aware of any correspondent relationships in non-banking sectors? If so, do you consider those relationships to be risky and should the requirements in section 29 also apply to those correspondent relationships?	
Money or value transfer service providers	
4.112. If you are an MVTS provider which uses agents, how do you currently maintain visibility of how many agents you have?	No comments
4.113. Should a MVTS provider be required to maintain a current list of its agents as part of its AML/CFT programme?	
4.114. 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)?	

4.115. Should the Act explicitly state that a MVTS provider is responsible and liable for AML/CFT compliance of any activities undertaken by its agent? Why or why not?	
4.116. If you are an MVTS provider which uses agents, do you currently include your agents in your programme, and monitor them for compliance (including conducting vetting and training)? Why or why not?	
4.117. Should we issue regulations to explicitly require MVTS providers to monitor and manage its agents for compliance with its AML/CFT programme (including vetting and training obligations)? Why or why not?	
4.118. What would be the cost implications of requiring MVTS providers to include agents in their programmes?	
4.119. Who should be responsible for the AML/CFT compliance for sub-agents for MVTS providers which use a multi-layer approach? Should it be the MVTS provider, the master agent, or both?	
4.120. Should we issue regulations to declare that master agents are reporting entities under the Act in their own right? Why or why not?	
4.121. What would be the cost implications of requiring MVTS providers to include agents in their programmes?	
New technologies	
4.122. What risks with new products or technologies have you identified in your business or sector? What do you currently do with those risks?	ASB recommends: - An explicit requirement to perform a risk assessment in relation to new products or technologies launched. - This should be underpinned by regulations and supported by guidance outlining what good practice looks like in this space (potential utilising examples)
4.123. 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?	
4.124. If so, should the risks be assessed prior to the launch or use of any new products or technologies?	
4.125. What would be the cost implications of explicitly requiring businesses to assess the risks of new products or technologies?	
4.126. Should we issue regulations to explicitly require businesses to mitigate risks identified with new products or technologies? Why or why not?	
4.127. Would there be any cost implications of explicitly requiring business to mitigate the risks of new products or technologies?	
Virtual asset service provider obligations	
4.128. Are there any obligations we need to tailor for virtual asset service providers? Is there any further support that we should provide to assist them with complying with their obligations?	No comments.
4.129. Should we set specific thresholds for occasional transactions for virtual asset service providers? Why or why not?	
4.130. If so, should the threshold be set at NZD 1,500 (in line with the FATF standards) or NZD 1,000 (in line with the Act's existing threshold for currency exchange and wire transfers)? Why?	
4.131. Are there any challenges that we would need to navigate in setting occasional transaction thresholds for virtual assets?	
4.132. Should we issue regulations to declare that transfers of virtual assets to be cross-border wire transfers? Why or why not?	
4.133. Would there be any challenges with taking this approach? How could we address those challenges?	
Wire transfers	
4.134. What challenges have you encountered with the definitions involved in a wire transfer, including international wire transfers?	ASB recommends that consideration be given to:

4.135. Do the definitions need to be modernised and amended to be better reflect business practices? If so, how?	- **Operational impact of reducing the wire transfer limit below NZD1,000** – while system impact may prove relatively low, the amount of reporting traffic will be significant – particularly for entities without systematised solutions. - **Foreign Exchange Transaction** – give consideration to removing these from being in scope of reportability. - **Allow CDD Programme to be relied upon:** Require that information be verified to the extent performed under the CDD Programme (thereby allowing for historically verified customers to be uplifted under general OCDD – rather than setting an expectation to refresh prior to process wire transfers. - **Intermediary Institution Exemption** (see PTR response)
4.136. Are there any other issues with the definitions that we have not identified?	
4.137. What information, if any, do you currently provide when conducting wire transfers below NZD 1000?	
4.138. Should we issue regulations requiring wire transfers below NZD 1000 to be accompanied with some information about the originator and beneficiary? Why or why not?	
4.139. What would be the cost implications from requiring specific information be collected for and accompany wire transfers of less than NZD 1000?	
4.140. How do you currently treat wire transfers which lack the required information about the originator or beneficiary, including below the NZD 1000 threshold?	
4.141. Should ordering institutions be explicitly prohibited from executing wire transfers in all circumstances where information about the parties is missing, including information about the beneficiary? Why or why not?	
4.142. Would there be any impact on compliance costs if an explicit prohibition existed for ordering institutions?	
4.143. When acting as an intermediary institution, what do you currently do with information about the originator and beneficiary?	
4.144. Should we amend the Act to mandate intermediary institutions to retain the information with the wire transfer? Why or why not?	
4.145. If you act as an intermediary institution, do you do some or all of the following: • keep records where relevant information cannot be passed along in the domestic leg of a wire transfer where technical limitations prevent the information from being accompanied? • take reasonable measures to identify international wire transfers lacking the required information? • have risk-based policies in place for determining what to do with wire transfers lacking the required information?	
4.146. Should we issue regulations requiring intermediary institutions to take these steps, in line with the FATF standards? Why or why not?	
4.147. What would be the cost implications from requiring intermediary institutions to take these steps?	
4.148. Do you currently take any reasonable measures to identify international wire transfers that lack required information? If so, what are those measures and why do you take them?	
4.149. Should we issue regulations requiring beneficiary institutions to take reasonable measures, which may include post-event or real time monitoring, to identify international wire transfers that lack the required originator or beneficiary information?	
4.150. What would be the cost implications from requiring beneficiary institutions to take these steps?	
Prescribed transaction reports	
4.151. Are the prescribed transaction reporting requirements clear, fit-for-purpose, and relevant? If not, what improvements or changes do we need to make?	ASB supports additional clarity with regard to reportability of transaction. Scenarios include: - **Local Payments for Trade Transactions (exports and imports) for foreign and local currency.** <u>Strict Literal Interpretation of the Act</u> The Act defines International Wire Transfers and considers them in scope for reporting under PTR. Key characteristics are:
4.152. Have you encountered any challenges in complying with your PTR obligations? What are those challenges and how could we resolve them?	
4.153. Should we issue regulations or a Code of Practice to provide more clarity about the sorts of transactions that require a PTR?	
4.154. 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?	

4.155. Should non-bank financial institutions (other than MVTS providers) and DNFBPs be required to report PTRs for international fund transfers?	Wire Transfers are transactions carried out on behalf of a person (the originator) through a reporting entity by electronic means with a view to making an amount of money available to a beneficiary (who may also be the originator) at another reporting entity International Wire Transfers are where: At least one of the ordering, intermediary or beneficiary institutions are in New Zealand and At least one of the ordering, intermediary or beneficiary institutions are outside of New Zealand Under this interpretation, instances where foreign currency is both involved and necessitates the flow of funds through non-domestic correspondent banks (e.g. USD via BNY), it's arguable that the flow is reportable. <u>Risk-based Interpretation</u> In 2017, in response to questions posed by the industry in the lead up to PTR, the FIU gave advice on the following scenario: Both the ordering institution and beneficiary institution are based in New Zealand, but an intermediary institution is based outside of New Zealand. This scenario often occurs when the currency is not in NZD. The chain of funds transfer involves an international intermediary bank. Does NZ FIU expect reporting entities to report transactions in this scenario? The FIU responded saying that these wouldn't be reportable. I understand that it was on this basis that the project excluded such payments from the current PTR framework. There is no formal FIU/RBNZ document or publication which states this – just a file note maintained from the industry engagement at the time (in 2017) In addition, this scenario was discussed at a PTR workshop on 8th July, where it was acknowledged that the approach adopted by participants in the industry was varied and it was accepted that the payments would be of limited intelligence where they are reported. - **PTR Reportability where there is a chain of reporting entities** – additional clarity sought on who should report and who is not required to. Consider refining the definition of ordering institution. - **Bulk Funding Payments & Credit Card Transactions** - **ISO20022 implications for PTR** – ensure changes are considered in uplift definitions/obligations
4.156. If so, should the PTR obligations on non-bank financial institutions and DNFBPs be separate to those imposed on banks and MVTS providers?	
4.157. Are there any other options to ensure that New Zealand has a robust PTR obligation that maximises financial intelligence available to the FIU, while minimising the accompanying compliance burden across all reporting entities?	
4.158. Should we amend the existing regulatory exemption for intermediary institutions so that it does not apply to MVTS providers?	
4.159. Are there any alternative options that we should consider which ensure that financial intelligence on international wire transfers is collected when multiple MVTS providers are involved in the transaction?	
4.160. Are there any other intermediary institutions that should be included in the exemption?	
4.161. 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?	
4.162. Do you consider that a lower threshold for PTRs to be more in line with New Zealand's risk and context? If so, what would be the appropriate threshold for reporting?	
4.163. Are there any practical issues not identified in this document that we should address before changing any PTR threshold?	
4.164. How much would a change in reporting threshold impact your business?	
4.165. How much time would you need to implement the change?	
Reliance on third parties	
4.166. Do you use any of the reliance provisions in the AML/CFT Act? If so, which provisions do you use?	Nothing in addition to comments raised in CDD Section.
4.167. Are there any barriers to you using reliance to the extent you would like to?	
4.168. Are there any changes that could be made to the reliance provisions that would mean you used them more? If so, what?	
4.169. Given the "approved entities" approach is inconsistent with FATF standards and no entities have been approved, should we continue to have an "approved entities" approach?	
4.170. If so, how should the government approve an entity for third party reliance? What standards should an entity be required to meet to become approved?	

4.171. If your business is a reporting entity, would you want to be an approved entity? Why or why not?	
4.172. Are there any alternative approaches we should consider to enable liability to be shared during reliance?	
4.173. Should we issue regulations to enable other types of businesses to form DBGs, if so, what are those types of businesses and why should they be eligible to form a DBG?	
4.174. Should we issue regulations to prescribe that overseas DBG members must conduct CDD to the level required by our Act?	
4.175. Do we need to change existing eligibility criteria for forming DBGs? Why?	
4.176. Are there any other obligations that DBG members should be able to share?	
4.177. Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD: • consider the level of country risk when determining whether a third party in another country can be relied upon; • take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and • be satisfied that the third party has record keeping arrangements in place.	
4.178. Would doing so have an impact on compliance costs for your business? If so, what is the nature of that impact?	
4.179. Are there any other issues or improvements that we can make to third party reliance provisions?	
4.180. Are there other forms of reliance that we should enable? If so, how would those reliance relationships work?	
4.181. What conditions should be imposed to ensure we do not inadvertently increase money laundering and terrorism financing vulnerabilities by allowing for other forms of reliance?	
Internal policies, procedures, and controls	
4.182. Are the minimum requirements set out still appropriate? Are there other requirements that should be prescribed, or requirements that should be clarified?	ASB does not support mandating that the AML CO be at a Senior Management level due to the fact that this might have unintended consequences for smaller firms. The principle that must apply is that the AML CO must be sufficiently experienced, resourced and senior within the firm in order to discharge their obligations. Consideration might also be given to mandating a degree of independence (i.e. by having a dotted reporting line to the Board etc.)
4.183. Should the Act mandate that compliance officers need to be at the senior management level of the business, in line with the FATF standards?	
4.184. Should the Act clarify that compliance officers must be natural persons, to avoid legal persons being appointed as compliance officers?	
4.185. If you are a member of a financial or non-financial group, do you already implement a group-wide programme even though it is not required?	
4.186. Should we mandate that groups of financial and non-financial businesses implement group-wide programmes to address the risks groups are exposed to?	
4.187. Do we need to clarify expectations regarding reviewing and keeping AML/CFT programmes up to date? If so, how should we clarify what is required?	
4.188. Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system?	
4.189. What other improvements or changes could we make to the independent audit or review requirements to ensure the obligation is useful for businesses without imposing unnecessary compliance costs?	
Higher-risk countries	
4.190. 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	**Specific Additional Requirements**: The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 in Ireland – which transposed the 5th EU Money Laundering Directive

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?	introduced specified ECDD measures (prescribed under law) where High Risk Countries where involved including: o Obtaining additional information on the customer and on the beneficial owner o Obtaining additional information on the intended nature of the business relationship o Obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner o Obtaining information on the reasons for the intended or performed transactions o Obtaining the approval of senior management for establishing or continuing the business relationship o 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
4.191. Should we issue regulations to impose proportionate and appropriate countermeasures to mitigate the risk of countries on FATF's blacklist?	
4.192. If so, what do you think would be appropriate measures to counter the risks these countries pose?	
4.193. Is the FATF blacklist an appropriate threshold? If not, what threshold would you prefer?	
4.194. 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?	
4.195. 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?	
4.196. How can we protect the rights of bona fide third parties?	
4.197. Should there be a process for affected parties to apply to revoke a countermeasure once made? If so, what could that process look like?	
Suspicious activity reporting	
4.198. How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?	ASB recommends the following with respect to suspicious activity reporting: - **Sharing within Group:** The Act should allow for the sharing of information pertaining to SARs within a Group structure for the purposes of managing ML/TF risk accordingly. - **Sharing Externally:** 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. - **Clarity on Timeframes:** ASB would welcome further clarity on the timeframe point by which SARs need to be submitted, particularly with regard to the 'inherently or objectively suspicious cases.
4.199. What barriers might you have to providing high quality reporting to the FIU?	
4.200. Should the threshold for reporting be amended to not capture low level offending?	
4.201. Should we expand the circumstances in which SARs or SAR information can be shared? If so, in what circumstances should this information be able to be shared?	
4.202. Should there be specific conditions that need to be fulfilled before this information can be shared? If so, what conditions should be imposed (e.g. application to the FIU)?	
4.203. Should we issue regulations to state that a MVTS provider that controls both the ordering and beneficiary ends of a wire transfer is required to consider both sides of the transfer to determine whether a SAR is required? Why or why not?	
4.204. If a SAR is required, should it be explicitly stated that it must be submitted in any jurisdiction where it is relevant?	
High value dealer obligations	
4.205. Should we extend additional AML/CFT obligations to high value dealers? Why or why not? If so, what should their obligations be?	No comments on this.
4.206. Should all high value dealers have increased obligations, or only certain types, e g., dealers in precious metals and stones, motor vehicle dealers?	
4.207. Are there any new risks in the high value dealer sector that you are seeing?	
Part 5 - Other issues or topics	
Cross-border transportation of cash	
5.1. Should the AML/CFT Act define the point at which a movement of cash or other instruments becomes an import or export?	No comments raised.
5.2. Should the timing of the requirement to complete a BCR be set to the time any Customs trade and/or mail declaration is made, before the item leaves New Zealand, for exports, and the time at which the item arrives in New Zealand, for imports?	
5.3. Should there be instances where certain groups or categories of vessel are not required to complete a BCR (for example, cruise ships or other vessels with items on board, where those items are not coming off the vessel)?	

5.4. How can we ensure the penalties for non-declared or falsely declared transportation of cash are effective, proportionate, and dissuasive?	
5.5. Should the Act allow for Customs officers to detain cash even where it is declared appropriately through creating a power, similar to an unexplained wealth order that could be applied where people are attempting to move suspiciously large volumes of cash?	
5.6. If so, how could we constrain this power to ensure it does not constitute an unreasonable search and seizure power?	
5.7. Should BCRs be required for more than just physical currency and bearer-negotiable instruments and also include other forms of value movements such as stored value instruments, casino chips, and precious metals and stones?	
Privacy and protection of information	
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?	ASB supports the full consideration of privacy regime in uplifting the AML/CFT Act and recommends full consultation with 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?	
5.12. Is the process for testing assertions that a document or piece of information is privileged set out in section 159A appropriate?	
Harnessing technology to improve regulatory effectiveness	
5.13. What challenges or barriers have you identified that prevent you from harnessing technology to improve efficiencies and effectiveness? How can we overcome those challenges?	As noted in our response above on CDD, it is important that the development of digital ID Service Trust Framework legislation, and supporting rules, have as a baseline, alignment with AML/CTF 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.
5.14. What additional challenges or barriers may exist which would prevent the adoption of digital identity once the Digital Identity Trust Framework is established and operational? How can we overcome those challenges?	
Harmonisation with Australian regulation	
5.15. Should we achieve greater harmonisation with Australia's regulation? If so, why and how?	No comments.
Ensuring system resilience	
5.16. How can we ensure the AML/CFT system is resilient to long- and short-term challenges?	No comments.

Minor Changes		
Definitions and terminology		
Issue	**Proposal for change**	**ASB view**
Life insurer is not currently defined in the AML/CFT Act; however, the definition of life insurance policies is by cross reference to the Insurance (Prudential Supervision) Act 2010.	Define life insurer in the AML/CFT Act by reference to the Insurance (Prudential Supervision) Act 2010.	No comments.

The meaning of the exclusion of "cheque deposits" in the definition of occasional transaction in section 5 of the AML/CFT Act is unclear. It is intended to apply to a deposit by cheque made at a bank or non-bank deposit taker, such that it does not trigger an occasional transaction by the person making the deposit with the bank. However, this is not specified.	Limit the exclusion of cheque deposits only to deposits made at a bank, non-bank deposit taker, or similar institution in line with the original policy intent.	No comments.
The definition of a DBG allows a group of 'related' DNFBPs, and their subsidiaries, that are reporting entities (within the same sector), to form a DBG with each other. 'Related' is intentionally not defined and DIA as the supervisor has issued guidance to assist DNFBPs understand how this should be interpreted. The Act appears to currently require subsidiaries to also be reporting entities to join a DBG., which is not the policy intent.	Propose that a DBG may be formed amongst a group of related reporting entities within a DNFBP sector and may also include a subsidiary of one of those DNFBPs in New Zealand (that is not a reporting entity).	No comments.
Section 114 of the AML/CFT Act is intended to convey the importance of the functions under the Customs and Excise Act 2018 in supporting the AML/CFT system but the current drafting does not clarify how the functions operate together.	Clarify and tidy up the sections to ensure the functions can clearly operate together.	No comments.
Information sharing		
Issue	**Proposal for change**	**ASB view**
Several key Acts are currently not included under section 140 of the AML/CFT Act. This limits data and partnerships across agencies and is preventing full environment assessments. The key agencies responsible for the listed legislation have observed money laundering and other harms but are currently unable to share information with the AML/CFT agencies.	Issue regulations to include additional Acts within the scope of section 140 to enable broader information sharing, such as: Commerce Act 1986, Corrections Act 2004, Criminal Proceeds (Recovery) Act 2009, Defence Act 1990, Environment Act 1986, Immigration Act 2009, and Trust Act 2019.	No comments.
Supervisors are empowered under section 48 to disclose personal information relating to employees or senior managers for law enforcement purposes and for the purpose of detecting, investigating, prosecuting any offence under specific Acts. Some Acts are not listed which limit the ability for some information that AML/CFT agencies hold to be shared for other regulatory purposes.	Add the following Acts to section 48(b) to improve clarity of the section and enable appropriate information sharing: Financial Markets Conduct Act 2013, Non-bank Deposit Takers Act 2013, Insurance (Prudential Supervision) Act 2010.	No objection in principle but would recommend engagement with Privacy Commissioner and ensure that disclosure of information is only permitted for legitimate and controlled purposes.
There are limited provisions explicitly allowing DIA to share information internally for law enforcement purposes (as defined in section 5). DIA administers other relevant legislation and it is not clear whether the AML/CFT function within DIA is able to share information with the teams responsible for the legislation listed above or vice versa.	Add further Acts to section 137(6) & (7) to clarify the ability for DIA to use information obtained as AML/CFT supervisor in other capacity and vice versa, e.g. Passport Act 1992, Births, Deaths, Marriages and Relationship Registration Act 1995, Citizenship Act 1977.	
There is no explicit provision in the AML/CFT Act which allows supervisors to conduct enquiries on behalf of foreign counterparts. Section 132(2)(e) of the AML/CFT Act provides a general power to initiate and act on requests from overseas counterparts, but not specifically conduct enquiries.	Clarify that supervisors are empowered to conduct enquiries on behalf of overseas counterparts.	No comments
SARs and PTRs		
Issue	**Proposal for change**	**ASB view**

No agency has the explicit function of ensuring compliance with SAR obligations. This function is not specifically listed as part of the functions of the AML/CFT Supervisors in section 130 (but supervisors are required to monitor for compliance more generally). Similarly, the Commissioner of Police is empowered to provide feedback to reporting entities on the quality and timing or their SARs and enforce the requirement to report.	Clarify which agencies are responsible for supervising compliance with SAR obligations.	ASB is supportive of clarity on supervision of compliance with SAR obligations – would recommend that this be a regulatory agency rather than law enforcement.
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.	Amend the regulation to obtain both the location of the account and the address of the sender to capture all relevant country information.	No objection in principle so long as ISO20022 implications are appropriately considered.
Exemptions		
Issue	**Proposal for change**	**ASB view**
Regulation 24AC of the AML/CFT (Exemptions) Regulations 2011 exempts reporting entities from certain sections obligations when subject to a production order or order issued under section 143(1)(a). However, reporting entities also receive orders under the Customs and Excise Act 2018 which may inadvertently lead to tipping off. In addition, in the process of complying with the relevant order, the reporting entity may form suspicions about associated persons. The exemption does not explicitly cover associates and therefore there is a risk that suspicious associates are tipped off.	Expand the exemption to also exempt reporting entities subject to an order issued under section 251 of the Customs and Excise Act 2018 as well as in respect of any suspicious associates who are identified in the process of complying with the relevant order.	No comments.
Regulation 17 AML/CFT (Exemptions) Regulations 2011 exempts reporting entities that are not an insurance company who are providing a service under a premium funding agreement from section 14-26 of the AML/CFT Act but does not exempt them from the requirement to identify a customer under section 11. This means exempt reporting entities must conduct ongoing CDD and account monitoring under section 31, but as they have not conducted CDD they have nothing to review.	Link the exemption more directly to the level of ML/TF risk associated with premium funding and clarify intention (or not) to capture premium funding as an activity for the purposes of AML/CFT	
Regulation 22 of the AML/CFT (Exemptions) Regulation 2011 exempts debt collection services from the AML/CFT Act other than relating to suspicious activity reporting. Debt collection services are defined as "the collection of debt by a person other than the creditor to whom it is owed or, where it has been assigned, to whom it was originally owed". The scope of this definition is unclear.	Clarify that the definition of debt collection services only relates to the collection of unpaid debt rather than the collection of any funds owed by one person to another.	
Regulation 9 of the AML/CFT (Exemptions) Regulations 2011 currently exempts currency exchange transactions performed in hotels that do not exceed NZD 1000 from most obligations in the Act, except obligations to file suspicious activity reports and keep records of any reports filed. However, the way this exemption operates may cause confusion for hotel operators which could be exploited by people seeking to launder money or finance terrorism. In particular, hotel operators may not be aware that they have full obligations for any currency exchange transaction	Clarify that the exemption applies to hotel providers which only undertake currency exchange transactions below NZD 1000.	

that exceeds NZD 1000, irrespective of how regularly they engage in any large value currency exchange transaction.		
Offences and penalties		
Issue	**Proposal for change**	**ASB view**
AML/CFT supervisors can issue a formal warning for failure to comply with AML/CFT requirements. However, calling these "formal warnings" does not necessarily carry the intended weight with the sector.	Replace "Formal warnings" with "Censure" to indicate the weight of the action. Censure is much more than a warning and includes a mandatory action plan.	No comments
There are two civil liability acts not explicitly included in section 78 of the Act. These are 1) failing to submit a suspicious activity report; 2) failures in respect of a risk assessment. It is also currently unclear whether 3) failing to submit an annual report to an AML/CFT supervisor is a civil liability act.	Amend section 78 to include these compliance breaches as civil liability acts.	
Preventive Measures		
Issue	**Proposal for change**	**ASB view**
Businesses are required to "have regard" to the factors set out in section 58(2) when conducting a risk assessment. This includes any applicable guidance material produced by AML/CFT supervisors or the Police, such as the National Risk Assessment or the various sectoral risk assessments. However, the language of "have regard to" could allow businesses to consider, but ultimately reject, government advice about national or sectoral risks and therefore fail to implement appropriate controls.	Amend section 58(2) to ensure that a business' risk assessment reflect government advice about national and sectoral risks.	No objections from ASB on this proposal. Additional guidance on good practices across high, medium and low impact businesses would also be welcomed.
In various sections of the AML/CFT Act, where a requirement for CDD is triggered outside a business relationship, there is reference to a customer seeking to conduct an occasional transaction or occasional activity. A person (outside a business relationship) becomes a customer if they conduct or seek to conduct an occasional transaction or occasional activity.	Replacing the term 'customer' with 'person' in sections 14(1)(b), 18(1)(b), 22(1)(b), 22(1)(b)(ii), 22(2)(b), and 22(5)(b) to align with the definition of customer in section 5.	No comments.
Businesses do not have an explicit obligation to verify any new information obtained through ongoing CDD, except where enhanced CDD is triggered.	Issue a regulation which explicitly requires businesses to verify any new information obtained through ongoing CDD.	ASB recommends that this be limited to instances where the new information changes the risk profile of the customer.
Section 37 applies prohibitions if a reporting entity "is unable to" conduct CDD in accordance with the AML/CFT Act. One reading of this is that if a reporting entity can conduct CDD as required, but merely chooses not to, the prohibitions do not apply.	Replace "is unable to" with "does not" in section 37 to ensure the prohibitions apply in all appropriate instances where CDD is not conducted.	If the obligation is to perform it and a reporting entity chooses not to adhere to that obligation, is this not non-compliance? No objections to the proposed change.
Simplified CDD is intended to apply only in situations where there are proven lower risks. There is no explicit requirement for businesses to not apply simplified CDD measures where there are higher risks, including where there is a suspicion of money laundering or terrorism financing.	Issue a regulation which states that simplified CDD is not appropriate where money laundering or terrorism financing risks are high or if there is suspicion of ML/TF.	Supported – included in CDD responses.
Businesses are not required to keep records of prescribed transaction reports.	Issue a regulation which requires businesses to keep records of prescribed transaction reports for five years.	No additional comments.
Section 52 of the Act states that records must be kept in written form in English or in a form to make them readily available. This	Amend section 52 to clarify that records must be made available immediately (e.g. upon request from a supervisor).	

means, but does not explicitly state, that records must be available immediately, or upon request.		
The Act does not set out how long businesses should retain account files, business correspondence, and written findings.	Issue a regulation which requires businesses to retain account files, business correspondence, and written findings for five years.	
There is no requirement that copies of records must be stored in New Zealand, particularly copies of customer identification documents.		
There is currently no requirement for ordering institution to maintain records about beneficiary's account number or unique transaction reference number.	Require ordering institutions to keep records on beneficiary account number or unique transaction numbers.	
It is currently not clear that wire transfer obligations apply to an underlying customer for MVTS providers that use agents.	Issue a regulation stating that the originator or beneficiary of a wire transfer is the underlying customer, not the MVTS provider's agent.	No comments.
There is a current Ministerial exemption in place that enables members of a DBG (that are reporting entities) to share a compliance officer, subject to certain conditions. The intent is to reduce compliance burden across members of a DBG.	Amend the Act to allow members of a DBG to share a compliance officer.	ASB is supportive of this change.