aml

From: [redacted]@securities.org.nz>
Sent: Friday, 10 December 2021 3:34 pm
To: aml
Cc: [redacted]
Subject: AML/CFT Submission from Securities Industry Association
Attachments: SIA submission MOJ_AML CFT review 101221.pdf; SIA submission MOJ_AML CFT review 101221.docx

Kia ora MOJ Team

Please find our cover letter and submission responses **attached**. You are welcome to get in touch with any questions or if you would like further information.

Kind regards

[redacted] | **Executive Director**
Securities Industry Association
[redacted]@securities.org.nz |www.securities.org.nz

10 December 2021

AML/CFT Consultation Team
Ministry of Justice
SX 10088
Wellington 6140

By email: aml@justice.govt.nz
CC: [redacted]@justice.govt.nz

Dear AML/CFT Consultation Team

Securities Industry Association submission: Review of the AML/CFT Act Consultation Document

Please find attached the submission prepared by the Securities Industry Association (**SIA**) in response to the Consultation Document: *Review of the AML/CFT Act (Ministry of Justice, October 2021).* Thank you for the opportunity to present our comments on this consultation paper.

About SIA
SIA represents the shared interests of sharebroking, wealth management and investment banking firms that are accredited NZX Market Participants.

SIA members employ more than 500 accredited NZX Advisers, NZDX Advisers and NZX Derivatives Advisers, and more than 400 Financial Advisers nationwide. The combined businesses of our members work with over 300,000 New Zealand retail investors, with total investment assets exceeding $80 billion, including $40 billion held in custodial accounts. Members also work with local and global institutions that invest in New Zealand.

No part of this submission is required to be kept confidential. Note, some SIA member firms may make an individual firm submission based on issues specific to their firm's business. Those issues and views may not be reflected in this submission.

We would also welcome an opportunity to meet with your team early in 2022 to provide further context to the responses in this submission.

If you have any questions about this submission or require further information, please get in touch.

Yours faithfully

[redacted]
Executive Director
SECURITIES INDUSTRY ASSOCIATION
[redacted]@securities.org.nz
www.securities.org.nz

Institutional arrangements and stewardship

Please be advised that SIA responses are provided in light blue.

1.1. Are the purposes of the Act still appropriate for New Zealand's AML/CFT regime or should they be changed? Are there any other purposes that should be included other than what is mentioned?-

1.2. Should a purpose of the Act be that it seeks to actively *prevent* money laundering and terrorism financing, rather than simply deterring or detecting it? -

1.3. If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there need to be any additional or updated obligations for businesses? -

1.4. Should a purpose of the Act be that it also seeks to counter the financing of proliferation of weapons of mass destruction? Why or why not?-

1.5. If so, should the purpose be limited to proliferation financing risks emanating from Iran and the Democratic People's Republic of Korea or should the purpose be to combat proliferation financing more generally? Why?-

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? -

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

SIA suggests that consideration should be given to a centralised database or approach to verifying information. Please refer to our submissions in section 4.

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?-

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?

SIA believes in order to achieve workable legislation, there needs to be a balance between taking prescriptive and risk-based approaches. Where legislation is less prescriptive in some areas, it allows a reporting entity, via its AML Programme and the AML Compliance Officer, an opportunity to define if and when they will allow an exception to the customer due diligence (CDD) process in relation to the relative risk. For example, in circumstances where an older person was unable to provide current photographic identification.

However, without sufficient best practice examples across the industry and a well-regulated community of auditors to assist with that, a risk-based approach can be difficult to apply in practice.

Overall, we believe the Act strikes an appropriate balance between prescription and a risk-based approach, but this needs to be better supported by guidance and auditors.

1.10. Do some obligations require the government to set minimum standards? How could this be done? What role should guidance play in providing further clarity?-

1.11. Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?

SIA is aware that the law is not applied consistently or rigorously in some industries or areas, where information does not require the same degree of verification and scrutiny as our members. We support high standards, but they should be applied equally to everyone who operates within the framework. More communication and guidance on best practice is required to ensure consistency.

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?

The Financial Action Task Force recommended that exemptions should only be given if there is a low risk of AML/CFT. SIA strongly suggests that the legislation needs to recognise that some risk is acceptable and ensure that there are clear guidelines so that this can be applied fairly and consistently.

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

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

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

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

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

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

1.21. Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done? -

1.22. How could the regime better protect the need for people to access banking services to properly participate in society? -

1.23. Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them?

The unintended consequences of the current regime are the burdens placed on:

a) customers – who are required to meet CCD obligations in a world that is increasingly difficult to do this both in person or electronically, and repeatedly required to do it for many people, e.g. their bank, broker, lawyer. Customers also lose an aspect of financial privacy.

b) business – many are already working to high compliance standards have to manage the customer relationship and their experience and expectations and bear the ongoing cost of the compliance system requirements.

A streamlined electronic identify verification system would remove the burden for both. Please refer to our submissions in section 4.

1.24. Can the Act do more to enable private sector collaboration and coordination, and if so, what?

We suggest that the legislation could recognise AML processes undertaken by licenced intermediaries, regardless of where the transaction instructions come from.

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?

SIA suggests there would be advantages to sharing more information about the AML/CFT landscape and how the Act is working effectively. Advisers spend significant time following processes and protocol to ensure they meet requirements; however, there is no apparent evidence of it working. For example, how it is preventing AML or other crime. It would also be worthwhile to receive feedback that it is working, and perhaps sector reports and evidence on what is it is preventing and protecting.

All industries can learn from better understanding threats in the wider environment and having confidence in the systems that eliminate them.

It would also be useful in ensuring it is applied appropriately within firms. We also suggest that there is more sector-specific education and training. For example, FIU training focuses mainly on cash-based firms such as car dealers and real estate agents; however, we would appreciate information, education and training relevant to financial advice firms.

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

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

1.30. Should the FIU be able to request information from businesses on an ongoing basis? Why or why not? -

1.31. If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected? -

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? -

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

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

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?

Codes of Practice are useful for reporting entities; the fact that only one has been issued to date suggests that the current arrangements are not effective. SIA believes that a centralised and operational decision-maker is appropriate.

In addition, SIA believes that the requirement in s 67(2) (to expressly opt-out to the supervisor to the extent that equally effective measures are adopted) is onerous and discourages innovation. The requirement should just be that any opt-outs are recorded in the AML programme (where the auditor can then review them).

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?

SIA submits that Explanation Notes to Verification Codes of Practice are not an efficient way to regulate because there are too many materials for

reporting entities to navigate. They are a clunky tool, and version control is not always well managed by the regulators. The requirement to adhere to these Explanation Notes versus taking them into consideration in a risk assessment is unclear and inconsistently applied.

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?

Yes, SIA believes they could provide clarity over inconsistently applied Guidance Notes and would aid version control if rules were all in one document. They would provide clear guidance to auditors and clarity over standards imposed by audit firms. However, such Rules should operate as a 'safe harbour' rather than on a mandatory compliance basis to allow for reporting entities to take a risk-based approach.

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?

We would suggest an experienced body for issuing and maintaining standards of a related and similar nature, for example, Chartered Accountants Australia and New Zealand.

1.47. Would you support regulations being issued for a tightly constrained direct data access arrangement which enables specific government agencies to query intelligence the FIU holds? Why or why not? -

1.48. Are there any other privacy concerns that were not taken into consideration in the Privacy Impact Assessment that you think should be mitigated? -

1.49. What, if any, potential impacts do you identify for businesses if information they share is then shared with other agencies? Could there be potential negative repercussions notwithstanding the protections within ***section 44***?-

1.50. Would you support the development of data-matching arrangements with FIU and other agencies to combat other financial offending, including trade-based money laundering and illicit trade? Why or why not? -

1.51. What concerns, privacy or otherwise, would we need to navigate and mitigate if we developed data-matching arrangements? For example, would allowing data-matching impact the likelihood of businesses being willing to file SARs? -

1.52. 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?

A registration scheme would be useful to other reporting entities, for example, to allow them to check that an entity is aware that it has responsibilities under the Act.

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?

SIA does not believe there is any merit in introducing an additional licensing regime for reporting entities. Supervisors would already have visibility of reporting entities through registration. In addition, the audit requirement gives an element of self-policing. With an associated cost, licensing would add significantly to the compliance cost of Firms with no parallel benefit. If a licensing regime is to be considered, we believe that this can only happen with a single regulator for a consistent approach to this self-regulating model.

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?

The benefit of these new regimes would accrue to the economy generally rather than reporting entities; as such, SIA believes that the government, not reporting entities, should bear the costs.

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? -

Scope of the AML/CFT Act

2.1. How should the Act determine whether an activity is captured, particularly for DNFBPs? Does the Act need to prescribe how businesses should determine when something is in the "ordinary course of business"? -

2.2. If "ordinary course of business" was amended to provide greater clarity, particularly for DFNBPs, how should it be articulated? -

2.3. Should "ordinary" be removed, and if so, how could we provide some regulatory relief for businesses which provide activities infrequently? Are there unintended consequences that may result?-

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?

The reference to "participating in securities issues and the provision of financial services related to those issues" has caused uncertainty; the FMA provided guidance in 2012 but this referred to the Securities Act 1978, which has since been repealed. It is not clear why, for example, merely providing financial advice on a securities issue should be a financial institution activity.

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? -

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

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

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

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

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

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?

SIA suggests preparing account and tax statements should attract AML/CFT obligations, as it is an opportunity to identify ML/FT at source. Where there are red flags, such as a lack of evidence for financial transactions and inconsistent information, the preparer should be obligated to identify the source of funds they are reporting. Although financial records are prepared for the holder, it is widely accepted that they are used as evidence of income by many agencies and industry.

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

We propose that obligations could be similar to other AML/CFT reporting entities. For example, based on the level of risk, increasing verification requirements and red flag reporting internally, with FIU reporting for suspicious activity.

2.37. Should tax-exempt non-profits and non-resident tax charities be included within the scope of the AML/CFT Act given their vulnerabilities to being misused for terrorism financing? -

2.38. If these non-profit organisations were included, what should their obligations be? -

2.39. 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? -

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? -

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? -

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? -	

2.56. Should the AML/CFT Act define its territorial scope? -

2.57. If so, how should the Act define a business or activity to be within the Act's territorial scope? -

Supervision, regulation, and enforcement

3.1. **Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it?**

SIA questions whether three supervisors are necessary, as our experience is that guidance and views from the different supervisors can vary. This not only causes confusion but can also hinder the production of effective guidance.

The legislation itself and the way it is written is relatively straightforward; however, that is part of the issue. AML/CFT is very complex, and with so many supervisors, it is challenging to apply it consistently. Due to its importance from a FATF perspective, SIA suggests that it would be beneficial to have more clarity from the Supervisors by way of examples of best practice.

The lack of guidance from the FMA makes it difficult for SIA members to justify to their customers what must be done and why and that this is industry best practice. There is a perception that different markets have different levels of security and supervision.

We also question whether there is enough sharing of information between the Supervisors and with the FIU.

A single regulator would help address all of these issues.

3.2. **If it were to change, what supervisory model do you think would be more effective in a New Zealand context?**

We support a single supervisory entity for consistency. It appears to be too difficult to reach a consensus on some issues with multiple agencies involved. A single supervisor would improve the quality and timeliness of all aspects of supervision.

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?**

SIA is concerned by the lack of consistency across reporting entities with respect to how AML/CFT obligations are being met. The apparent absence of consistency across the three Supervisors manifests in the lack of consistency by which AML processes are undertaken. For example, there appears to be a variety of approaches for the use of outsourced AML providers.

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?**

Due to the simple way the Act is written, it is open to interpretation, and therefore, there appears to be no consistency in its application across various industries. At a minimum, more structured, regulated auditors could apply consistent standards to the audits of the participants.

A single regulator would have suitable critical mass and power to generate change in the AML/CFT environment and have a better chance of increasing best practice standards and future-proofing the approach to technology.

For example, applications such as RealMe have access to the passport photo database and can verify a customer using a smartphone, but these databases are not open to commercial or wider use. A single supervisor could focus efforts to ensure this could be opened up in a safe and secure way. Other activities could be explored in tandem, for example, getting banks on board to share and verify data by progressing the Open Banking / Consumer Data Right regime.

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

3.6. Should AML/CFT Supervisors have the power to conduct onsite inspections of reporting entities operating from a dwelling house? If so, what controls should be implemented to protect the rights of the occupants? -

3.7. What are some advantages or disadvantages of remote onsite inspections?

There are concerns with the proposal to give Supervisors remote powers of inspection. The SIA's strong preference is that reporting entities are only required to provide direct and remote access to relevant information. It should also be noted that it may not be possible in all cases to provide remote access to all data and systems.

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?

We believe there should be a streamlined process where all of the entities are in NZ and are wholly-owned subsidiaries of the same holding company.

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

3.11. Should explicit standards for audits and auditors be introduced? If so, what should those standards be and how could they be used to ensure audits are of higher quality?

SIA supports flexibility and the ability to apply a risk-based approach; however, there is material inconsistency across audit firms, audit reports, and how they apply the guidance, making it difficult to implement the requirements effectively. There appears no level of consistency, yet we are all trying to do the right thing.

The level of skill varies between audit firms and often differs from the Supervisor's approach and findings. There is no qualification or standard

for auditors, and this could mean varying degrees of quality standards, processes or scrutiny being met. We strongly suggest auditors need accreditation to ensure they are all working to the same high standard. Our members use accredited auditors, but we know others don't.

SIA strongly believes auditors need to have qualifications and standards that are independently reviewed and assessed. AML audit firms need to operate to a high standard and should be monitored and licensed. We understand that currently, it is acceptable for an audit to be undertaken by a non-AML qualified auditor.

We also suggest standardising the audit process and templates so you could benchmark a firm against another.

3.12. Who would be responsible for enforcing the standards of auditors?

The Supervisor(s).

3.13. What impact would that have on cost for audits? What benefits would there be for businesses if we ensured higher quality audits?

The additional costs would be largely borne by those currently using sub-par auditors, which is appropriate. In terms of benefits, consistent application of the expectations of the regulators by audit firms would reduce the perceived competitive advantage of any businesses that are not applying the same high standard of AML standards.

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?

This should apply equally to consultants as to audit firms. There are a significant number of 'consultants' in the industry with varying levels of qualifications and experience, and this again leads to complete inconsistency in compliance across the market.

3.17. Who would be responsible for 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? -

3.21. Does the existing penalty framework in the AML/CFT Act allow for effective, proportionate, and dissuasive sanctions to be applied in all circumstances, including for larger entities? Why or why not? -

3.22. Would additional enforcement interventions, such as fines for non-compliance or enabling the restriction, suspension, or removal of a licence or registration enable more proportionate, effective, and responsive enforcement? -

3.23. Are there any other changes we could make to enhance the penalty framework in the Act? -

3.24. Should the Act allow for higher penalties at the top end of seriousness to ensure sufficiently dissuasive penalties can be imposed for large businesses? If so, what should the penalties be? -

3.25. Would broadening the scope of civil sanctions to include directors and senior management support compliance outcomes? Should this include other employees?

We note the legislation is clear as to which obligations the penalties link to, and this should be reserved for gross misconduct or fraudulent activity. However, we submit that employees, including compliance officers, should be excluded. The risk of including all employees is that entities will struggle to resource these roles as applicants will feel the need for relevant qualifications, even across the more procedural AML tasks, and New Zealand's compliance resource market is too small to support this. We need to make sure that the scope is meeting its intended needs but not causing unintended consequences.

The intent to do the right thing should not be penalised. This change should not be considered before the inconsistencies in guidance, supervisor application, auditors and consultants are completely resolved and operating effectively.

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?

Everyone should be provided protections when acting in good faith.

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

3.29. Should we change the time limit by which prosecutions must be brought by? If so, what should we change the time limit to? -

Preventive measures

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

SIA members face a number of challenges in this regard.

Duplication in verification processes

There is often duplication in the process for clients who require their ID to be verified or certified. For example, consider a situation when an Adviser in an NZX Participant Firm is opening an account or a client and verifying the client's identification face-to-face. If the client then wants to open a bank account, in that case, the bank will not accept the ID the Adviser has verified, as financial advisers do not meet the criteria for a "trusted referee" per the Amended Identity Verification Code of Practice 2013. This becomes a significant issue for the client who is then required to either get their ID certified by a Justice of the Peace, or similar, or present themselves in person to the bank. Banks now have fewer branches and are operating with limited opening hours, which is difficult for clients.

A centralised AML verification database is needed

SIA strongly believes that Government needs to centralise the AML verification process to allow a single 'source of truth' for ID verification purposes. For example, a digital AML passport that shows an individual has been validated by the Government, rather than having each individual reporting entity conducting due diligence, which often means for a single transaction, a person may end up providing the same documents multiple times.

It is not uncommon to find scenarios where a person is buying a home requires at least six different entities to conduct Customer Due Diligence (CDD) on them, i.e. real estate agent, bank, insurance company, KiwiSaver provider, sharebroker, lawyer.

Electronic or online verification through a centralised 'single source of truth' would make this process seamless, save time for all entities and the consumer, and ensure a robust CDD process. Entities that have access to this database would need to be trusted, for example, FMA-regulated and licensed Financial Advice Providers.

With non-face-to-face onboarding becoming increasingly common, a reliable method of linking the presenter to the claimed identity is essential. At a minimum, the Government should open up the DIA passport and NZTA drivers' licence photo databases to access by third-party software developers to facilitate linking the presenter and the claimed identity. Currently, RealMe accesses the DIA database for these purposes, but this functionality is not available to the wider market. Without these tools, the private sector is significantly hindered.

Standard account naming conventions

The banking system is increasingly used as an alternative means of linking the presenter and the claimed identity, with intermediaries relying on control of a bank account in the name of the claimed identity as establishing a link to the presenter. However, this process is not as robust as desirable because the account name that the client's bank passes to the intermediary's bank does not follow a standard naming convention and, in addition, is often limited to 20 characters, which is often insufficient to hold the full account name.

It would be highly advantageous to all parties if a standard account naming convention was introduced and any character limitations removed. This would provide a better system for intermediaries to verify client details and ensure that all account names established followed a standardised approach from a point in time. A single regulator would be well placed to strongly influence this change.

Move to electronic verification

Most businesses activity is on online platforms. There is very little business transacted in hard copy. Soft copy and e-signatures are commonplace and accepted for contracts.

The notion of certified copies of documents is becoming increasingly irrelevant and redundant and is not fit for purpose for how we operate today. Clients who required certified copies over COVID-19 lockdowns found this process immensely difficult. Non-face-to-face means of verification are required. However, the supervisor guidance appears to hold such means to a higher standard than 'wet ink' certification, which itself has significant vulnerabilities (see below). Further to this, it is difficult to onboard new customers when you cannot meet face-to-face. Smartphone technology should be embraced as a tool to support this process.

Cumbersome certification, room for error and document chasing

If an NZX Participant Firm cannot meet a client in person to verify their identity, the client must provide 'wet ink' certified identification and address verification. Whilst unintentional, the certification is often not completed satisfactorily by trusted referees, who generally have received no training in relation to certification of documents. For example, the referee only signs and dates the document and omits their name or designation, the certification is not dated, or it is certified by someone not recognised to do so. This means the Firm must ask the client for another certified copy that meets the guidelines, and this becomes a cumbersome process.

All of this creates difficulty for law-abiding clients, but none whatsoever for those looking to fraudulently open accounts. For example, for most kinds of 'trusted referees', there are no means by which an intermediary can verify that the certification was, in fact, carried out by the referee.

Further, the Supervisor's guidance is that an original certified document is also required, which can take several days to arrive by post. This drawn-out

process is not a positive experience for the client and causes unnecessary staff time checking the post and following up with the client to see if they have posted the document. This does not get the business relationship off to a good start as part of the onboarding process.

Institutional clients – simplify due diligence

In addition to retail investor clients, SIA members work with a range of institutional clients, from listed entities eligible for simplified due diligence to large, well-known companies owned by a family trust that require enhanced due diligence.

SIA suggests that simplified due diligence should apply to the broader group of institutional clients. If a Firm requests ID for an employee of an institutional client (where that employee is acting on behalf of the client), 'privacy grounds' are often cited in response to the request. The client will usually then provide a 'letter of comfort' or Board resolution to confirm the relevant staff have authority to act on behalf of the client, and/or that the client is compliant with the relevant AML/CFT requirements and will provide copies of their employee's IDs to regulators if required. SIA would appreciate clarification of the adequacy of this approach or whether simplified due diligence could be considered appropriate to the risk.

Ongoing Due Diligence Processes

SIA members appreciate the need for maintaining up-to-date information to mitigate against fraud and risk; however, we seek clarification on what this might look like in the future.

Investment in technology infrastructure

SIA suggests that there needs to be investment in the development of technology infrastructure to support changes to the verification process that will bring about better efficiencies and benefits for businesses and consumers, and ultimately make identity fraud and AML/CFT more difficult.

A centralised system that provides 'one source of truth', would reduce costs, time and effort for businesses and consumers across New Zealand, increasing efficiency, confidence and reducing risk.

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?

As noted above, the key shortcomings of current AML systems and technology infrastructure are:

1. the lack of progressing a digital identity standard, and
2. the lack of standardisation/conventions for bank account names.

New Zealand is increasingly verifying identity online – we have moved away from cash and cheques to electronic transactions, and the face-to-face nature of communication and transactions for many tasks such as paying bills and banking is in the past.

It should be possible to easily verify an account name against an image, especially using the current technology and systems.

As noted above, SIA suggests that the Department of Internal Affairs and NZ Transport Agency need to make their respective photo databases available for this purpose to approved businesses so that these can be more widely utilised as a verification process.

Furthermore, it is perplexing that we still have to rely on the integrity of the banking system for AML identity verification, and this process has not been modified to make this more streamlined for users of this system, nor any alternatives provided. It is currently hindered by a 20 character limit. If standard account name conventions were introduced, it would provide a more accessible and accurate way to match customer information.

If two transformative actions could make the AML process more streamlined and more robust for customers and businesses, it would be establishing a common standard for account names and linking to an open banking service.

An open banking service would allow key pre-approved customer information/data to be more easily shared between banks and approved businesses or access to a single validated repository of information.

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? -

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?

SIA believes that the obligation to verify address should be removed from the Act. This obligation can represent a significant barrier to younger people accessing financial services (as they often will have no readily available documentary link to their current place of residence) while presenting no difficulties at all to those who are actually looking to launder money (as they can quite easily rent an apartment and get utilities connected at the premises, thereby obtaining proof of address).

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?

Nature and Purpose

SIA suggests that legislation and guidance need more flexibility on how some businesses collect information on nature and purpose. For example, some entities such as wealth managers will know more about their clients and have a longer-standing relationship than other businesses.

In these circumstances, collecting 'nature' and 'purpose' on top of what is already required to be recorded for other legislative obligations is essentially asking for the same information but in a format that suits the AML

process. There should be recognition that some advice processes may already cover the requirements for AML, so in those instances, flexibility should be given over 'ticking the box' by allowing Firms to formulate their procedures so they can show how they are meeting the obligation.

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? -

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

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

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?

Verifying source of funds and source of wealth

Clients often get offended or think firms are interrogative when the source of funds/wealth documentation is required. This is particularly the case with long-term clients who wish to introduce new funds for investment and are then required to prove the source of funds.

Clients are comfortable with verbally advising where the funds have come from; however, when firms require further evidence of the source, clients feel that they are not trusted.

This process also causes confusion for customers and businesses, as it is not clear how far do you go to verify the source. For example, there could be a long passage of time since the source of wealth was generated, such as the sale of a family farm 20 years ago, where evidence or records are limited. This can be a source of angst or friction for clients. We are also aware that there are inconsistencies in market practices due to the lack of clarity.

SIA suggests that consideration could be given to allowing discretion for long-standing clients or those well-known to a reporting entity, particularly in low-risk clients undertaking low-risk transactions.

More generally, SIA agrees that regulations or guidance to prescribe when information on source of wealth or funds (or both) is required would be useful. This would avoid inconsistencies in the approach between reporting entities and the prospect of provider-shopping by clients. This

result could possibly also be achieved through better guidance from the Supervisors.

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?

SIA proposes there should be a level of reliance on the system in place, such that proof of source of funds from a New Zealand bank is sufficient evidence, for example, a Term deposit. The approach should also be risk-based, and source of wealth not required where a lower risk entity has an ECDD requirement. These are matters that could be specified in the reporting entity's risk assessment and AML programme.

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

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? -

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

Yes, the definition is unclear. It has two limbs, whereas the guidance effectively rewrites the definition into three limbs, none of which correspond to the two in the Act. Many believe the definition in the Act to be the result of a drafting error.

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

The Act should adopt the approach of the guidance.

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? -

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? Yes, SIA believes it would be useful for this to be clarified by regulation. It would be important to clarify that 'indirect control' of the customer means control generally, not just control in relation to the transaction being undertaken (for example, a client directing a stockbroker to undertake a securities transaction would not be a beneficial owner for these purposes). 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? We believe the appropriate route would be to consult on the need for the exemption once the proposed amendment to the Act was finalised, as it is possible that the amendments to the Act would not cover all of the use cases for the exemption. 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? Based on the information provided, the change would likely not require significant changes to existing processes, and so the additional compliance costs would likely not be significant.	
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? We believe a Code of Practice would provide a useful safe harbour for reporting entities. 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? SIA believes a Code of Practice would provide a useful safe harbour for reporting entities. 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. **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?**

Currently, it appears that regulators are far removed from real-world practices and technology solutions. For example, recent FMA guidance refers to posting a document. As referred to elsewhere in this submission, electronic options should be considered as appropriate in certain circumstances.

We need a commitment from the government to implement workable solutions; for example, engaging with banks for standard account name conventions or fast-tracking open banking solutions would be a logical step.

Verification requirements should be proportionate to risk profile

SIA believes AML verification obligations should be conducted according to the risk profile. However, regulation currently takes a conservative approach and is therefore interpreted very conservatively, which renders it ineffective. Furthermore, when guidance is provided too late, it is also inadequate.

The criteria to meet current verification requirements in some circumstances are simply not proportionate to the risk. As a result, the compliance burden on firms to meet those requirements is disproportionate to the risk. For example, SIA members as NZX Participant Firms and as licensed Financial Advisers work to very high compliance levels, meet external accountability and audit standards through robust processes and record-keeping, and operate to high responsibility standards. These high standards help mitigate risk, as does knowing our customers and understanding the risk spectrum. However, long-standing customers of Firms are required to jump through hoops to prove who they are regularly.

At the same time, it is possible that less professional operators in other industries may lack audit systems or are 'softly' audited by a close contact. Through the nature of their work and how they work, they may be operating with higher risk.

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

SIA agrees with the observations in the consultation paper about the IVCOP. It works only for simple use cases, but these are generally not the ones with high ML/FT risk.

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

4.47. **Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g. verifying name and date of birth of high-risk**

customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?

Yes, SIA believes that this would be useful for reporting entities.

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

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

As noted elsewhere in this submission, there are a number of challenges in relation to the use of electronic verification. The IVCOP is outdated in this regard; the supervisors have attempted to supplement it with guidance, which is confusing and difficult to apply. There is an urgent need not only for reform of the IVCOP in this regard but also for the Government to take practical steps to ensure that the infrastructure required is available, for example, by ensuring that DIA/NZTA photo databases are opened up to third-party providers, and that bank account names follow a standardised format (see our responses to questions 4.1 and 4.2).

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

As noted in our response to question 4.18 above, SIA does not believe that the requirement for addresses verification should continue. Official documents, such as passports, do not connect to an address.

It is difficult to understand the value the requirement to verify a residential address adds to the AML/CFT regime. Putting it simply, it would be easy for a criminal to fake an address. This aspect of the process presents another burden to customers and businesses yet doesn't pose any real difficulty or deterrent to a criminal.

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

SIA submits that address verification should not be mandatory. We support adopting the Australian model where reporting entities can elect to verify date of birth or address but not require either.

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

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

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

SIA suggests that New Zealand's regime needs to align with international practices. It is not clear how certification in accordance with an offshore

jurisdiction's requirements fits with the identity verification code of practice (IVCOP).

Specifically, section 11 of the IVCOP requires certification to include a statement linking the form of identification to the person who presented. However, this is not always required overseas and therefore omitted from documents certified in accordance with the laws of another jurisdiction.

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

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

Yes, where the entity is subject to AML/CFT regulation itself (in NZ or a reputable foreign jurisdiction), the AML/CFT officer of the client (or their foreign equivalent) should be able to verify the identity/authority information on behalf of the client.

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

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

Vehicle for holding personal assets

SIA submits that the legislation does not need the "vehicle for holding personal assets" classification in the definition of EDD (section 22(1)(a)(i)). Under the recent amendments relating to nominee shareholders and directors, investment companies that have hidden beneficial ownership will be caught. A New Zealand company established for an individual to hold their wealth is only risky if there are nominees, shareholders, or directors.

Enhanced CDD on family trusts

SIA believes that simple NZ-based Family Trusts with clear beneficial owners and real individuals as Trustees should be treated like the individuals behind them and only subject to ECDD if other higher risk factors are present. Very simple family trusts can consume a significant amount of time for negligible benefit to the AML/CFT system.

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

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

We suggest Trusts that have an overseas Trust as the beneficial owner should require enhanced CDD. We believe such trusts would better be

identified by guidance rather than legislation or regulation. Reporting entities could be required to incorporate the relevant criteria and assessment programmes in their AML programmes.

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

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

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

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

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

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

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

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

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

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

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

Currently, ongoing CDD is required on a material change in the business relationship and insufficient information. We strongly disagree with the proposal to remove the word "material". A change in the business relationship that is not material is not indicative of money laundering or financing terrorism.

The cost to businesses to implement changes to meet the wider definition would be significant and a financial burden to Firms. Furthermore, it would potentially reduce customers' access to financial services if changing their services gives rise to a significant administrative burden. It may also deter customers from changing services or switching services, which is not in the customer's best interest.

We do not believe the 'sinking lid' approach is workable either. The current approach allows businesses to take a flexible approach to re-papering accounts based on the circumstances and risk.

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

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

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

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

4.76. Do you have any challenges with complying with your record-keeping obligations? How could we address those challenges? -

4.77. Are there any other records we should require businesses to keep, depending on the nature of their business? -

4.78. Does the exemption from keeping records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold hinder reconstruction of transactions? If so, should the exemption be modified or removed?-

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

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

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

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

Extension of definition of Politically Exposed Persons (PEP) to include NZ PEPs

SIA does not agree that the definition of PEPs should include domestic PEPs, as we are not sure this is warranted given New Zealand's bribery and corruption reputation, more specifically its low risk. However, if this proceeds, we would expect the legislation to recognise that not all new Zealand PEPs are high risk or subject to EDD.

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

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

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

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

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

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

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

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

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

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

4.93. If we include domestic PEPs and PEPs from international organisations within scope of the Act, should the Act allow for business to take reasonable steps, according to the level of risk involved, to determine

whether a customer or beneficial owner is a domestic or international organisation PEP? -

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

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

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

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

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

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

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

4.101. What support would businesses need to conduct this assessment? -

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

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

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

4.105. How should businesses receive timely updates to sanctions lists? -

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.123. What would be the cost implications of requiring MVTS providers to include agents in their programmes? -	
4.124. Who should be responsible for the AML/CFT compliance for sub-agents for MVTS providers which use a multi-layer approach? Should it be the MVTS provider, the master agent, or both? - 4.125. Should we issue regulations to declare that master agents are reporting entities under the Act in their own right? Why or why not? - 4.126. What would be the cost implications of requiring MVTS providers to include agents in their programmes? -	
4.127. What risks with new products or technologies have you identified in your business or sector? What do you currently do with those risks? - 4.128. Should we issue regulations to explicitly require businesses to assess risks in relation to the development of new products, new business practices (including new delivery mechanisms), and using new or developing technologies for both new and pre-existing products? Why or why not? - 4.129. If so, should the risks be assessed prior to the launch or use of any new products or technologies? - 4.130. What would be the cost implications of explicitly requiring businesses to assess the risks of new products or technologies? -	
4.131. Should we issue regulations to explicitly require businesses to mitigate risks identified with new products or technologies? Why or why not? - 4.132. Would there be any cost implications of explicitly requiring business to mitigate the risks of new products or technologies? -	
4.133. Are there any obligations we need to tailor for virtual asset service providers? Is there any further support that we should provide to assist them with complying with their obligations? -	
4.134. Should we set specific thresholds for occasional transactions for virtual asset service providers? Why or why not? - 4.135. If so, should the threshold be set at NZD 1,500 (in line with the FATF standards) or NZD 1,000 (in line with the Act's exiAct's threshold for currency exchange and wire transfers)? Why? - 4.136. Are there any challenges that we would need to navigate in setting occasional transaction thresholds for virtual assets? -	
4.137. Should we issue regulations to declare that transfers of virtual assets to be cross-border wire transfers? Why or why not? -	

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

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

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

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

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

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

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

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

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

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

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

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

4.150. If you act as an intermediary institution, do you do some or all of the following:

- keep records where relevant information cannot be passed along in the domestic leg of a wire transfer where technical limitations prevent the information from being accompanied? -
- take reasonable measures to identify international wire transfers lacking the required information? -
- have risk-based policies in place for determining what to do with wire transfers lacking the required information? -

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

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

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

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

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

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

Prescribed Transaction Report (PTRs)

SIA submits that FMA guidance that excludes FMA regulated entities from the PTR rules is enshrined in the new legislation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

When purchasing a business that is a reporting entity, it is common for the purchaser to rely under section 33 on the vendor's previously-undertaken CDD.

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

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

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

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

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

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

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

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

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

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

4.182. Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD:

- consider the level of country risk when determining whether a third party in another country can be relied upon;
- take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and
- be satisfied that the third party has record keeping arrangements in place. -

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suspicious Activity Reporting (SAR)

We think the Suspicious Activity Reporting process is straightforward, although the Financial Intelligence Unit's (FIU) system is outdated.

EDD after Suspicious Activity Reporting

SIA submits that the requirement to do extended due diligence (EDD) after filing a SAR under section 22A has proven unmanageable from a practical perspective while avoiding tipping off. This is particularly true if a decision has already been made to close the account, as it raises flags to the client if we approach the client for further information then close the account. The risk of AML/CFT remains the same after the EDD is completed in that case. If this suggestion is not supported, we propose adding flexibility to close the account (subject to rule not to tip off), without requiring EDD in that case.

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

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

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

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

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

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

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

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

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

Other issues or topics

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

5.2. Should the timing of the requirement to complete a BCR be set to the time any Customs trade and/or mail declaration is made, before the 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? -

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?

Introducing a single source of identity verification could ensure that people can only access the information they are entitled to access; however that information could be trusted to be robust. Customers would also have more control over their data – and only have to verify it once or update as required as you would a driver's license or a passport. We refer to the MBIE Consumer Data Right consultation that would require high levels of information protection, but consumers have control over their data.

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? -

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?

The current verification processes are burdensome for customers.

Please refer to our submissions in section 4. In particular, SIA suggests that the Act needs to be updated to support an automated technology-based approach to AML and ensure that it is future-proofed to accommodate rapid changes that we can expect in this area.

An open banking system would allow for information to be shared more easily between authorised businesses. There could be restrictions on some information, and customers would have control over what was shared, but standard information could be shared to verify a consumer's identity. Banks would be the most logical source for this.

While this might take some time to establish, existing avenues could be utilised, such as the drivers' license and passport photo databases that could be used for visual verification.

There is currently limited scope for new technology-based product development, given there is limited shared access to customer information. There is variability in outsourced AML verification services, and given there is no standard practice customers or consistency in processes, some customers do not trust current electronic processes and are unsure if they are legitimate.

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?

A key obstacle would be businesses that currently wield a lot of power due to the volume of customers and information they hold, such as banks or insurance companies. However, this could be overcome by ensuring that the customer holds the power over their information and gives their permission for regulated and reputable businesses to access it. This could be once to meet basic CDD requirements and a case by case basis for other information.

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

There would be benefits to customers and businesses on both sides of the Tasman if New Zealand's AML/CFT regulations aligned with Australia's.

SIA supports mutual recognition of highly-regulated businesses, as it facilitates more trade and allows for economies and streamlined processes where there are frequent interactions.

If both countries are operating to the same high levels of regulation with similarly robust and aligned processes, we then have an Australasian standard that would potentially be recognised globally and facilitate safe global business practices with other jurisdictions.

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

SIA believes the legislation needs to accommodate the fast changes in technology and those that we are yet to see. The current legislation has New Zealand hamstrung with very little flexibility to do anything other than.

Engaging directly with industries and trusting their first-hand experiences is a sensible way to understand the current challenges and what might be perceived as challenges.

Good operators are already working to extremely high compliance standards, as trust, reliability, integrity and reputation are fundamental to the success of their business model. They cannot afford to take any risks, but they will embrace authorised technology and opportunities to bring efficiencies and enhanced protections for their customers and businesses.

If there is a robust regulatory framework in place, then a balanced principle- and risk-based approach allows for flexibility and good judgement at a business level.

Minor changes

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

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