aml

From: [redacted]@sharesies.co.nz>
Sent: Thursday, 16 December 2021 3:36 pm
To: aml
Cc: [redacted]
Subject: Re: Extension to time to submit on MoJ's AML/CFT review
Attachments: Final - AMLCFT Submission Letter (1).pdf

Hi Nick

Thank you for the extension of time which has allowed us to get a more comprehensive response together. Please find our response attached.

Chris and I are very open to answering any further questions that come up along the way.

Thanks again.

Irene

On Thu, Dec 2, 2021 at 9:50 AM aml <aml@justice.govt.nz> wrote:

> Kia ora Irene,
>
> Good to hear from you.
>
> Happy to accommodate a two week extension, but note that if it is at all possible to get it to us earlier that would be greatly appreciated 😊
>
> Ngā mihi,
>
> Nick
>
> MINISTRY OF JUSTICE
> Tāhū o te Ture
>
> [redacted]
> Kaitohu Tōmua | Senior Policy Advisor
> Criminal Law | Policy Group
> [redacted]
> www.justice.govt.nz

Mon Tues Wed Thur Fri

From: [redacted]@sharesies.co.nz>
Sent: Thursday, 2 December 2021 9:43 am
To: aml <aml@justice.govt.nz>
Cc: [redacted]@sharesies.co.nz>
Subject: Extension to time to submit on MoJ's AML/CFT review

Good morning

Could we please receive an extension on the due date to submit on the MoJ's AML/CFT review. We have a draft submission in progress but it would benefit from additional time to get more input from across our business. If possible a 2 week extension would be great.

Thanks

[redacted]

--

[redacted] • Senior Legal Counsel

[redacted]

sharesies.com • facebook.com/sharesies

16 December 2021

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

Kia ora,

Feedback on Review of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act)

Sharesies welcomes the opportunity to provide feedback on the Ministry of Justice (**MoJ**)'s review of the AML/CFT Act.

Who we are

Sharesies is a wealth development platform and our purpose is to create financial empowerment for everyone. Our vision is to give people with $5 and $5 million the same money opportunities. The Sharesies platform currently makes it possible for New Zealanders and Australians to invest in companies, funds and investment products listed in New Zealand, Australia and the US starting with as little as $0.01. As at the start of December 2021, Sharesies had over 500,000 investors signed up to the platform and nearly $2B invested for our investors.

What's important

Our submission focuses on the below three themes which are important to us and we believe important to New Zealand.

At Sharesies we really care about financial empowerment and believe this starts with access. We were heartened to see reference to financial inclusion in the MoJ's consultation paper. We strongly support the MoJ keeping financial inclusion in mind as it looks to strengthen New Zealand's AML / CFT regime. It's really important that stronger controls on ML/TF do not come at the cost of New Zealanders access to and legitimate participation in the financial system.

We are a proud Wellington business with global aspirations. We also love to see other New Zealand businesses grow and succeed internationally. The growth of Sharesies and other tech startups here in New Zealand grows the skills, talent and products that help New Zealand to participate in the global digital economy. We are passionate about it. We'd love to see this review take a really considered approach to ensuring that the new AML/CFT regime provides an even playing field for New Zealand companies competing with global corporations both here in New Zealand and internationally.

Relatedly, we are also super keen to see the new regime take advantage of the novel digital solutions that clever kiwi companies create. We'd like to see a regime that is sufficiently flexible to enable companies to create and implement new and better ways of managing ML/TF risks, particularly as those risks change as criminals take advantage of digital opportunities too.

In addition to expanding on the above themes, we also submit on a number of specific questions from the consultation document towards the end of our submission.

We can help, please keep in touch

As the MoJ's review progresses, we would appreciate the opportunity to take part in further consultation and industry engagement. Sharesies has always operated in a digital-first environment. Our model means we have a different perspective to traditional financial institutions. We believe we have much we could helpfully contribute to ensure the MoJ's review progresses with the digital future in mind.

We support a BIG aspiration for this review!

We support an aspiration for a best practice AML/CFT regime in New Zealand. We are concerned that the MoJ's stated aspiration to make New Zealand the hardest place in the world to ML/TF may make it challenging for the review to keep legitimate uses of the financial system in mind. We believe it's important that the review does not become blinkered to the majority (legitimate participants in the financial system) while focusing on regulation to manage the exceptional (ML/TF in the financial system). We're encouraged to see the reference to management of unintended consequences in the consultation document. We believe it's important for us to encourage the MoJ to take a sufficiently broad approach to the review. We'd love for the aspiration for the review to be broadened to include reference to financial inclusion and encouragement of novel digital solutions. We're hopeful that thoughtful, modern regulation can provide better protection against the risk of ML/TF, and have fewer unintended consequences for New Zealanders.

Please Prioritise Financial Inclusion 💖

We'd love to see the AML/CFT Act expressly seek to balance ML/TF risks with desirable outcomes in terms of financial inclusion. In addition to being fundamentally driven by financial inclusion and empowerment as a company, we are also concerned that financial exclusion can in turn increase the risk of undetected money-laundering. We believe that risk-based inclusivity should be the starting point for the regime and given appropriate deference in the AML/CFT Act.

More specifically, we also consider that the following elements of the current AML/CFT regime result in undesirable financial exclusion and require attention and future proofing in this review:

Options for low cost digital verification are limited to select New Zealand IDs

The options for digital customer due diligence (**CDD**) are essentially limited to holders of a New Zealand Driver's Licence or New Zealand passport. This is a limited subset of people in New Zealand. Who does it exclude?

- Young people - who are not of driving age, have chosen not to drive or who have not yet travelled internationally
- People who are less affluent, older or disabled - where driving and international travel may be less accessible
- New Zealand based people with foreign passports and foreign driver's licences.

Other modes of proving identity are prohibitively manual, costly and complex for a digital service to provide. Equally when signing up for a digital experience a customer reasonably expects digital verification and isn't willing to carry out a time intensive manual verification process. We believe it's reasonable to ask for legislation that enables New Zealand businesses to provide a digital verification option to nearly everyone in New Zealand. We also believe these options need to be future-proofed to enable continued digital innovation.

Address verification no longer makes sense

In an increasingly digital world using a physical address to prove who we are seems ever less necessary or relevant. Providing proof of address can be difficult for people sharing residences with others, people of no fixed address or people who move frequently. Again this tends to disproportionately impact the young and less affluent. We submit that it doesn't make sense to require address verification when other more reliable means of digital identity verification exist (and more options will become available).

In response to question 4.50, we submit that address verification places an unduly large burden on reporting entities, results in undesirable financial exclusion and provides little value in terms of preventing ML/TF. There is no reliable and universally acceptable form of address verification. Further, the existing requirement in New Zealand goes beyond what is required under the FATF standards, which only require address verification in limited circumstances. We suggest that the AML/CFT Act is amended at a minimum to pare back the requirement to be consistent with the FATF standards.

Enhanced Due Diligence on Trusts

Allowing standard CDD on low-risk trusts would ensure New Zealanders who hold assets in this common way are not excluded from access to low-cost digital financial services and would allow reporting entities to focus their resources and energy on higher risk customers. In response to question 4.58, we agree that simple family trusts should not require enhanced CDD due to their low ML/TF risk. We consider that the mandatory requirement to conduct enhanced CDD is contrary to the aim of having an AML/CFT regime that is proportionate to the ML/TF risk. This requirement presently perpetrates unjustified financial exclusion, because it is simply too hard and not financially justifiable for many financial institutions, including Sharesies, to complete enhanced CDD on these customers. Enhanced CDD is particularly difficult to complete or scale in a digital way; it requires human intervention. We are a digital business and rely on digitisation to scale and keep our services low cost to facilitate financial inclusion. Under the current regime it is not financially viable for us to extend our services to entities that require enhanced CDD - if we wish to keep our service priced at a rate that facilitates financial inclusion.

Please keep in mind the aspirations of legitimate New Zealand business 🌱

New Zealand businesses need an even playing field for competing with international companies at home and abroad

We consider that the AML/CFT Act needs to recognise its impact on the ability of New Zealand companies to compete with international companies both in New Zealand and abroad. This is increasingly important in a digitally connected world where international companies provide services to people in New Zealand and New Zealand companies provide services to people internationally.

As a proud Kiwi business, it is concerning to think of: (1) international companies providing services to New Zealanders without the burden of our AML/CFT Act regime, meaning we and other New Zealand companies don't have an even playing field at home; and (2) New Zealand companies being constrained by the New Zealand AML/CFT Act as we expand internationally, meaning there is never an even playing field for New Zealand companies with global aspirations. In implementing a regime significantly out of

step with our major trading partners, the MoJ would risk impeding the ability of New Zealand businesses to compete with the big players locally and globally.

New Zealand companies competing with international companies in New Zealand

As we become increasingly digitally connected, we see more international companies offering New Zealanders access to financial services online under a model where that company is operating under foreign law and wherever possible avoiding regulation by New Zealand legislation. As New Zealand companies increasingly compete against international companies here in New Zealand, it is important that New Zealand AML/CFT legislation is not materially more burdensome than the equivalent regimes of our major trading partners. A more balanced aspiration is to ensure New Zealand legislation offers protections against ML/TF at least equivalent to those of our major trading partners or that New Zealand is no more attractive to those seeking to ML/TF than in other established economies.

The consultation document asks for input about the benefit of harmonisation with Australia. We believe harmonisation (or mutual recognition) makes sense in Australasia given the high degree of integration of our economies, and the financial services sectors in particular. It would also create one less hurdle for New Zealand financial services businesses hoping to operate across the Tasman. As a digital financial institution with experience in considering the differences between New Zealand and Australian AML/CFT regimes, Sharesies is keen to remain part of the conversation around harmonisation (or mutual recognition) between the two countries. Models for solutions between New Zealand and Australia can be found in other sectors, such as food safety and securities offerings. The European Union also offers other models for harmonisation - including in anti-money laundering regulation.

New Zealand companies competing with international companies internationally

Sharesies is concerned with proposed amendments that may result in New Zealand companies having to comply with the AML/CFT regimes of multiple countries for a single customer. In particular, it would be concerning if the difference between the regimes meant that New Zealand businesses were required to ask for more or different information from its customers at on-boarding (or subsequently) when compared to competitors in another jurisdiction. We know from experience that adding one additional or different step in our sign up flow can have a material impact on sign up rates. In practice, if our on-boarding requirements (due to the reach of New Zealand AML/CFT requirements) were more onerous than a competitor in another jurisdiction, we would have to spend significantly more on advertising in order to bump up our advertising conversion to make up for a materially lower sign up conversion. In a digital world where ease of signing up and participating is essential, adding additional hurdles that are not common across competitors would be a material disadvantage to New Zealand companies looking to compete abroad.

Proportionate compliance costs to risks

We welcome and encourage changes to the AML/CFT Act to ensure that the compliance burden is proportionate to the risks to the economy and money laundering in New Zealand. We consider that the AML/CFT Act has been too prescriptive in a number of areas, such as requiring enhanced CDD on all trusts (regardless of the risk that the trust presents) and requiring reporting entities to obtain nature and purpose information at on-boarding regardless of whether this will help the entity to identify subsequent suspicious activity. We discuss each of these points further below. We consider that the AML/CFT regime needs to be proportional to the ML/TF risks for New Zealand's economy and in each instance proportional and targeted to the risks of specific entities.

Please modernise our regime to reflect and make way for the digital economy 💾

The AML/CFT Act needs to not only keep pace with, but encourage and promote, the innovation and advances of New Zealand's digital economy. We believe a digital first approach leads to improved outcomes for investors and provides greater financial empowerment to New Zealanders. We think it is important that the rules and regulations governing New Zealand business are modern and future proofed as the economy becomes increasingly digitised.

Less prescription - enable us to create digital solutions which reduce ML/TF risk

In general, the AML/CFT Act, Codes and the guidance issued by Supervisors are prescriptive and are now outdated in being geared towards traditional businesses that meet with customers physically. In addition, updates are typically too slow to keep pace with the innovations of digital businesses.

We encourage the development of a more purposive and less prescriptive approach to managing ML/TF risk for digital businesses. For example, for digital businesses, linking the connection of the person being dealt with online with the ID provided is presently difficult with limited options under the Act, IVCOP and guidance. However, digital businesses like Sharesies have alternative strong algorithmic risk based monitoring tools available - which we submit are more successful at reducing ML/TF risk than the prescriptive identity verification requirements in the current regime.

Less prescriptive law would enable businesses to innovate and apply the best way to reduce ML/TF risk in their own business model. As FATF itself has acknowledged, fostering digital innovation is most likely to reduce ML/TF risk.

An example of where prescription has not kept step with innovation - Nature and Purpose Questions

In response to question 4.18, Sharesies submits that asking a customer to provide information about the proposed nature and purpose of their relationship at the time of on-boarding should not be required under the AML/CFT Act. We believe this is one clear example of where the prescriptive requirements of the regime have not kept step with the innovations in scalable digital technology. It is a requirement that has resulted in a compliance and customer burden without a corresponding counter ML/TF benefit.

At Sharesies, we can predict to a high degree of certainty the expected behaviour of a customer based on information we collect in the ordinary course of our relationship and we monitor all transactions for the unexpected. We recognise that these questions can be useful in assisting some reporting entities to set account monitoring protocols to assess whether the claimed nature and purpose aligns with account activity in order to reduce the level of monitoring those entities need to undertake. However, at Sharesies we have highly scalable technology that enables us to monitor all accounts for suspicious activity. We do not need to ask funneling questions so as to monitor less activity. A person is of course unlikely to disclose an intention to ML/TF during the onboarding process. The questions we must ask and answers we receive are not necessary to shape how we can monitor for behaviour that may indicate a ML/TF risk.

We note that Recommendation 10 of the FATF Recommendations lists the relevant CDD measure as "[u]nderstanding and, *as appropriate*¸ obtaining information on the purpose and intended nature of the business relationship". We submit that flexibility could be built into this requirement in our regime to allow reporting entities to either obtain or otherwise understand the nature and purpose of the

relationship through other means (such as through predictive algorithms and account monitoring). This would allow the AML/CFT regime to leverage the innovations in scalable digital technology.

Guidance in practice has the status of law

In practice, guidance allows Supervisors to effectively change the law without a thorough democratic consultation process, and without wide input from relevant stakeholders. We believe this results in substandard outcomes. Guidance publicly sets the Supervisor's interpretation of the law and in order for a reporting entity to take a different approach that reporting entity must get comfortable with the prospect of being publicly censured by its Supervisor and a long costly road in court if they wish to debate another interpretation. This is a heavy burden on a reporting entity and in most instances simply not worth it from a reputational harm or cost perspective. In this way, guidance, in practice, comes to have the effect of law.

In addition, there is no clear process for a Supervisor to approve an alternative approach, or no formal process whereby a reporting entity can seek to have their supervisor get comfortable with an approach. 'Approval' is only obtained through non-objection, which is uncomfortable when trying to 'think outside the box'. It is very difficult for a reporting entity to get comfort that implementing an alternative solution won't result in later censure from its Supervisor. The public perception of a warning creates hesitancy in the sector for creating novel solutions. The overly prescriptive regime with highly prescriptive guidelines forces companies into narrow solutions and hampers the creation of novel digital solutions.

Challenges with the IVCOP

In response to question 4.45, we submit that the Identity Verification Code of Practice (**IVCOP**) presents many challenges for a digital first business, and does not serve the objectives of the AML/CFT regime well. The IVCOP primarily focuses on providing certified identity documents to reporting entities, with comparatively little consideration of electronic identity verification (**EIV**). The IVCOP should recognise EIV as the primary method of verifying a customer's identity as the digital economy develops. As a digital business, Sharesies uses EIV to complete CDD. Currently, the IVCOP provides a limited range of EIV methods and proposes methods to link a customer to their claimed identity that are unfit for a digital business.

Sources of EIV are limited by the Guideline

The *Explanatory Note: Electronic Identity Verification Guideline* (**Guideline**) issued by the AML/CFT Supervisors in July 2021 is overly prescriptive in providing which sources may be used to meet the requirements for EIV under the IVCOP.

The IVCOP permits a reporting entity to satisfy the EIV requirements from a single independent electronic source that can verify a customer's identity to a high level of confidence. However, the Guideline prescribes that only RealMe can meet this threshold. RealMe is costly to integrate with and costly to use. As it stands, RealMe is also not widely or confidently used by enough New Zealanders to provide a useful source of EIV for Sharesies. RealMe is also not a workable solution for international people in New Zealand. RealMe is not a solution we can use overseas, so the technical development effort required to integrate with RealMe is not something that can be reused as we expand internationally.

In addition, the Guideline provides that either the Confirmation Service run by the Department of Internal Affairs or the New Zealand Transport Agency database should be used by reporting entities

using two electronic sources to complete EIV. While the IVCOP itself provides some level of flexibility in choosing electronic sources, the Guideline suggests that the sources capable of meeting the IVCOP are very narrow, removing the flexibility provided. In addition, the level of prescription in the Guideline makes it difficult and uncomfortable for a reporting entity to claim that they are otherwise meeting the requirements of the AML/CFT Act if they are using other methods.

Additional methods required to link a customer to their claimed identity are not digital friendly

The methods suggested by the IVCOP to "link" a customer to the claimed identity are not suited to a digital business. The IVCOP suggests that reporting entities require a credit to be made from the customer's bank account which matches the name given to the reporting entity. However, the Guideline excludes use of BNZ (which excludes this as a method to link the very many New Zealanders who use a BNZ account) and includes use of Co-operative Bank (which makes no sense in a digital context because as far as Sharesies is aware the Co-operative Bank does not share customer account names digitally). So in practice a number of material New Zealand banking institutions are excluded from being used to digitally link a customer to their identity. This forces Sharesies, and other reporting entities, to consider other options in the IVCOP to link a customer to their claimed identity.

The other methods suggested in the Guideline include sending a bounce-back letter via the post to a customer's address with a unique code to return to the reporting entity. This method is slow and unrealistic to expect of a digital business and its customers. It is also unsophisticated in terms of the opportunity for interference and we believe easily rivaled by some of the digital options which the Guideline expressly states as insufficient. For example, the Guideline expressly provides that a video call with a customer showing their ID and face is not sufficient to link the person to their ID. We'd argue that the video option presents less ready opportunity for interference than the postal option which the Guideline expressly allows. A video call is arguably pretty comparable to a person presenting in person at a branch with their ID. A video call isn't a particularly viable option for Sharesies - despite being a digital solution it is obviously not scalable to have a human at the Sharesies end of every customer sign up. We use this example to note that the Guideline has a bias towards less digital and less viable options such as post.

For the regime to be workable there must be greater flexibility, less specificity and an avenue (but not a requirement - given that would slow down the opportunity for development) for reporting entities to get comfort that they are meeting their Supervisor's expectations. The current IVCOP and Guideline create an unacceptably high hurdle for digital onboarding of legitimate customers and no clear pathway for resolving this. We believe the Australian regime provides a useful example where the requirement is simply to "be reasonably satisfied that an individual customer is who they claim to be", without an overly prescriptive list of options on how this could be achieved and taking a risk based approach.

Remote Inspections - sounds good but please don't interfere with our tech

In response to questions 3.6 – 3.7, we welcome the use of remote inspections by Supervisors and consider that they could increase efficiency of inspections. However, given that interference with our technology and platform is a key concern with very high risk potential, we consider that the scope of the inspection should clearly exclude accessing our technology remotely.

Ongoing Customer Due Diligence requirements - must be achievable digitally

We consider that the Act should enable ongoing CDD requirements to be met by novel digital solutions. The more prescriptive the Act is, the less able we are to provide novel digital solutions. On-going CDD

should not require entities to repeat or reachieve the same level of CDD that is achieved at on-boarding. We should be able to rely on initial CDD as accurate and subsequent interactions (transaction monitoring and other system flags) to identify suspicious activity. In the ordinary course we have reasonable confidence that the due diligence completed at on-boarding remains accurate with transaction and other system flags picking up unexpected behaviour that might suggest further due diligence is required.

Assessment of New Technologies - its BAU please leave us to it

In relation to requiring Assessment of New Technologies in questions 4.128 - 4.130, Sharesies believes this would be an unnecessary compliance burden given general AML/CFT requirements apply to any such new technology. It's ordinary business for Shareises to consider the legal implications of launching new technology. Requiring a specific type of risk review for AML/CFT is a compliance burden without benefit. Businesses must comply with the general AML/CFT requirements including in relation to any new technology - there is no need for the law to dictate a process for how a business should go about this.

Record Keeping - keep in mind security implications

It would be useful to have clarity around what digital identity verification records a reporting entity must continue to hold. For example, if using biometric photo capture of peoples faces and their identity document (**ID**) do reporting entities need to keep photographs of both? If required to keep photos of peoples faces and ID this would appear to be an additional burden for digital businesses for which there is no equivalent when CDD is done physically - for example where a person shows their ID in a branch and a bank teller considers if the person presenting the ID is the person shown in the ID, our understanding is there is no physical record of photographs of both the person and their ID kept. We believe online CDD should equally be a point in time assessment (in this instance done by biometric technology rather than a bank teller) and that photo records of people's faces should not then need to be kept.

Section 50 of the AML/CFT Act requires a copy of the evidence or “if it is not practicable to retain” then “any information as is reasonably necessary to enable that evidence to be obtained”. It's not clear what amounts to “reasonably practicable” or who the reporting entity needs to ensure is able to obtain the evidence if it doesn't keep copies - is it the reporting entity or the FIU? Regardless, we believe requiring all entities that operate digitally to store digital copies of this information is high risk - particularly as more and more entities over time start using digital methods of identity verification. This could risk New Zealand becoming a greater target for data theft and identity fraud (in turn increasing ML/TF risks). Consumers are increasingly unhappy with these kinds of photos being taken or stored for long periods of time and there is a real technical compliance burden in storing these safely. Keeping these digital records safe is a costly and high risk enterprise that requires significant skill, it would be concerning to see a large number of companies required to keep hold of this information.

Other - random bits

Compliance Officers - leave us to structure ourselves please

In response to question 4.188, we don’t believe it is sensible to dictate that a compliance officer needs to be at the senior management level of the business. Organisational structure and AML/CFT risks vary across businesses. Businesses are best placed to determine where in the organisational structure the AML/CFT compliance officer should sit. A very low risk entity arguably does not need to have an

AML/CFT compliance officer sitting at the senior level. Equally, in a higher risk AML/CFT business it may make more sense for the AML/CFT officer to be someone who has an operational role dedicated to that cause rather than a senior leader holding this role with minimal time to attribute to the detail.

Across the jurisdictions in which Sharesies plans to operate, various laws impose requirements on our organisation's structure, sometimes with nonsensical outcomes and often with unintended people impact and unsettling restructuring. This proposed change would result in cost, complexity and people disruption that is not justified, because we don't believe it would materially reduce ML/TF risk. Without evidence of widespread non-compliance with the AML/CFT Act it would seem hard to justify adding a requirement aimed at ensuring compliance officer roles are high enough up the hierarchy to "ensure compliance".

Proportionate Penalties

In response to questions 3.21 - 3.22, we submit that the current range of penalties (such as formal warnings) is sufficient to sanction an entity because typically the primary concern (and financial impact) with any regulatory sanction is reputational damage. To justify a material increase in penalties or the introduction of fines, we believe there would need to be evidence of material or widespread non-compliance following the use of existing penalties such as public sanction. We expect there would be few instances where a reporting entity has had deficiencies publicly censured by a Supervisor and then continued to operate without correcting these.

To the extent that penalties are materially increased, we consider that these must be scaled to take into account the nature of the breach and the actual ML/TF risk or occurrence. Higher penalties should be reserved for the most serious offending. If there is a high penalty applied at a generic level we submit that the unintended consequence of this is to stifle innovation. Reporting entities may be warned off trying to provide novel solutions where the penalty is very high/generically high. This is more likely where it is not possible (or impractically slow) to get clarity as to whether a novel solution meets the Supervisor's expectations.

Personal liability

In response to question 3.25, we submit that any penalties imposed on employees, senior managers or directors need to have a clear application. In particular, the penalty should be clear what the person must do in order to avoid a penalty. For example, the penalties could be imposed:

- where there is knowledge by the senior manager: similar to the penalties proposed in the new Deposit Takers Act, where it is proposed that directors will be liable for false or misleading disclosure, with criminal penalties for knowing or reckless breaches; or
- where there is a failure to exercise due diligence to ensure compliance with the duties under the AML/CFT Act: similar to the new penalties for directors and senior managers under the Credit Contracts and Consumer Finance Act 2003 (CCCFA).

We also consider that if a penalty of this nature is imposed, the director or senior manager should be able to insure themselves against such a penalty (as is proposed in the new Deposit Takers Act).

Closing thoughts

Thanks for your time reviewing our submission, we'd like to keep in touch. Let us know if you have any follow up questions or if there is further industry consultation planned which we could helpfully contribute to.

Ngā mihi nui,

[redacted]
Senior Legal Counsel

[redacted]
AML/CFT Compliance Officer