aml

From: [redacted]@riskrobin.co.nz>
Sent: Friday, 3 December 2021 3:04 pm
To: aml
Subject: Submission in the Review of the AML/CFT Act - Claire Piper
Attachments: 3 December 2021- AML_CFT Act Consultation -CPiper.pdf

Hi there,

Please see attached.

[redacted]

Fodluh#Slshu
Vkh2Khu
354#589#4974
zzz1ulvnurelq1fr1q}

Submission in the Review of the AML/CFT Act

[redacted], *3 December 2021*
[redacted]*@riskrobin.co.nz*

The purpose of the AML/CFT Act

Primarily in response to questions 1.1; 4.203; 4.204; 4.206; 5.16
Associated with questions 1.2; 1.3; 1.24; 1.25; 1.26; 1.27; 1.30; 1.50; 3.21; 3.23

A consequence of the global AML/CFT compliance regime is that legislative police responsibilities are partially outsourced to the private sector. New Zealand businesses are now required to gather and report intelligence about potential criminal and terrorist activity to, and on behalf, of New Zealand police agencies.

From a New Zealand business' perspective, there are two types of compliance obligations enshrined in the AML/CFT Act;

- 'Type 1' compliance activities that constitute a methodology for *producing data* for the New Zealand Police, in the form of Suspicious Activity Reports (SARs) and Prescribed Transaction Reports (PTRs). Type 1 compliance activities concern a business' money laundering (ML) and terrorist financing (TF) risk. The intended purpose of these activities is to help New Zealand Police in their responsibilities; and

- 'Type 2' compliance activities that *demonstrate to regulators* that they are carrying out 'Type 1' compliance activities in the form of record keeping, audits, annual reporting, staff training, and other administrative tasks. Type 2 compliance activities concern a business' regulatory risk. The intended purpose of these activities is to help regulators monitor and enforce 'Type 1' activities.

The critical problems I've observed in working with hundreds of New Zealand reporting entities over the last eight years is:

- To be effective at detecting and deterring potential criminal and terrorist activity that give rise to ML/TF risk, people working in New Zeland businesses must be expert in such activity.

  They must be informed about historical, current, and developing predicate offences that give risk to ML/TF risk in the context of their business, they must

understand the nuances of suspicious red flags for each predicate offence, and they must assess the relevance, importance and urgency of each suspicious red flag before reporting meaningful intelligence to the New Zealand Police Financial Intelligence Unit (FIU).

Even if this were feasible, people tasked with this work are given negligible information, resources, and support from the FIU and regulators to even make attempts at engaging with it. Stale regulator-issued guidelines and generalised FIU monthly reports are not sufficient to help people working in businesses effectively engage with Type 1 compliance activities

- Directors of New Zealand businesses are almost exclusively concerned about and focussed on regulatory risk. This is logical, given all AML/CFT-related enforcement action to date has concerned businesses' *failures to demonstrate compliance*, not their failures to be effective at detecting and deterring ML/TF activity in their business. There is very little incentive to dedicate business resources to the actual purpose of the AML/CFT compliance regime;

- Businesses are given negligible evidence that any Type 1 compliance activities are impactful or relevant in any way. Data about the effectiveness of Type 1 compliance activities in New Zealand is not accessible and may not even exist (the FIU's monthly statistics reported in their monthly reports lack context and meaningful insight to improve the quality of Type 1 compliance activities).

  This further increases businesses' focus on Type 2 compliance activities which lack inherent meaning or purpose. This breeds contempt for the AML/CFT compliance regime within people in businesses and further disengages them from the critical nature of Type 1 compliance activities.

- Of the three specified purposes recorded in section 3 of the AML/CFT Act, only the second has a way of determining effectiveness - New Zealand's subjective performance in a Financial Action Task Force (FATF) evaluation can be measured. This specified purpose has the least import to, and impact on, New Zealand businesses and the New Zealand public.

  Without knowing how governmental agencies will assess the effectiveness of businesses detecting and deterring ML/TF activity, or how they will measure the associated impact on public confidence in the financial system, these specified purposes will remain flaccid and disregarded.

On this basis, I submit that;

- The purpose of the AML/CFT Act retains business' responsibility to detect and deter ML/TF activity. Introducing an additional active duty to *prevent* ML/TF imposes an even more unrealistic and unhelpful burden on businesses and people who are already unequipped to carry out specialist law enforcement duties.

- The legislation be updated to include methods of measuring the effectiveness of businesses detecting and deterring ML/TF activity, and the associated impact on public confidence in the financial system. This should incorporate data and information that demonstrate the extent to which AML/CFT compliance activities are, or are not, fulfilling these two purposes.

Risk-based approach to regulation

Primarily in response to question 1.7; 5.16
Associated with questions 1.9; 1.10; 1.11; 1.12; 1.13, 1.21; 1.27; 1.38; 1.39; 1.41; 4.1 to 4.71; 4.187; 4.192, 4.193; 4.195

Crime and terrorisim are inherently fast-moving and dynamic social phenomena, and New Zealand's AML/CFT risk framework must better be informed by this reality.

I submit that the supervisors' sector risk assessments (SRAs), and the FIU's national risk assessments (NRAs), do not help people working in New Zealand businesses to genuinely understand the nature of ML/TF threats, vulnerabilities, and risks impacting them. These documents are wildly generalised, quickly outdated, and easily provide prospective criminals and terrorists with a checklist of how to best avoid raising suspicion and detection.

For example, it is nonsensical that some businesses must currently benchmark their ML/TF risks according to the July 2017 Sector Risk Assessment by the Financial Markets' Authority (FMA). This document requires FMA supervised reporting entities to cite wildly outdated statistics and long-inaccurate generalised statements in their own risk assessments.

Sections 58 and 59 of the AML/CFT Act refer to reporting entities' obligation to maintain 'current' and 'up to date' risk assessments, with no such obligation imposed on supervisors or the FIU.

The qualitative risk assessment methodologies used by supervisors and adopted by most reporting entities are fallacious, outdated, and create misleading and empty conclusions about actual ML/TF risks impacting New Zealand at any one time. The methodologies used in SRAs confuse and conflate regulatory risk with ML/TF risk that lead to similar confusion and complexity within businesses.

This poor understanding and application of risk and risk assessments creates the following impacts;

- Undermines the trust and confidence of New Zealand businesses in the authority and competence of AML/CFT policy, regulatory, and police entities;

- Renders reporting entity risk assessments based on generic and outdated SRAs and NRAs inherently inaccurate and ineffective for the purposes of the AML/CFT Act.

  An inaccurate and ineffective risk assessment prevents reporting entities from developing the functional "risk-profile" necessary to engage with the risk-based regime. A functionally meaningless risk profile prevents reporting entities from making informed risk-based decisions when establishing a governance-level ML/TF and regulatory risk appetite, training staff, engaging compliance service providers, monitoring transactions, reporting SARs, and nearly all other risk-based compliance activities imposed on them.

  Critically, a functionally meaningless risk assessment and risk profile make it *impossible for businesses to meaningfully comply with sections 12 and 57 of the AML/CFT.*

  Where a meaningful and justifiable level of risk cannot be established, reporting entities cannot make effective and compliant decisions about standard and enhanced due diligence measures. They cannot design adequate and effective policies, procedures, and controls that are targeted to their risk assessment and risk profile. Auditors cannot make meaningful conclusions on the adequacy and effectiveness of policies, procedures, and controls that are not justified by a meaningful risk profile. And arguably, regulators are unable to carry out enforcement activities relating to sections 12 and 57.

- Further encouraging directors of businesses to priorise regulatory risks associated with compliance rather than ML/TF risks associated with real and relevant criminal and terrorist activity threats and vulnerabilties.

The existing risk framework enshrined by the AML/CFT Act is the foundational sepsis in the New Zealand AML/CFT compliance regime that can only beget rotten goods. Businesses cannot manage their costs of compliance, the public cannot be treated fairly, and government agencies cannot ethically enforce AML/CFT compliance obligations without a clear-eyed overhaul of the regime's approach to risk.

I submit that the legislation must be amended, wherever it is relevant, to encompass a rational and defendable risk framework that supports businesses to create functional risk profiles and provides an ethical basis for regulatory enforcement actions. I submit that nearly all questions in this consultation document cannot be sanely resolved without these changes.

It is impracticable for me to record my suggested approach for technical risk models in this document. I submit that this risk framework should be informed by the wealth of existing scholarship in operational and enterprise risk management. By way of indicative example, I offer the Committee of Sponsoring Organizations of the Treadway Commission's recent *Compliance Risk Management: Applying The Coso Erm Framework, November 2020* as an illustration of a modern and dynamic approach to compliance risk management,

Regulating auditors, consultants, and agents

Primarily in response to questions 3.11; 3.12; 3.14; 3.15; 3.16; 3.17; 3.19; 3.20
Associated with questions 4.194

I submit that the role of compliance service providers should be specified in legislation and be subject to a licensing and registration scheme. The purpose of the regime should be to;

- Encourage competent compliance service providers to demonstrate a standard of ethical professionalism and technical AML/CFT knowledge;

- Support businesses to make informed decisions about the competence of the compliance service provider they are engaging and to be clear on the scope and nature of their services;

- Enable supervisors to determine responsibility for poor compliance outcomes in monitoring and enforcement activities.

Compliance service providers should include;

- Technical specialists advising on AML/CFT strategy and documentation;
- Independent AML/CFT auditors;
- Customer onboarding agents including electronic identity verification (EIV) providers;
- AML/CFT training providers;
- Providers selling RegTech products such as transaction monitoring software, digital risk assessments, etc.

Professionals operating under other licensing regimes, such as legal and accounting service providers, should be required to be licensed as a compliance service provider before providing compliance services.

The Licensed Building Practitioner (LBP) Scheme under the Building Act 2004 provides a model for how different classes of licensing could operate. In that regime;

- It is clear what type of work requires different types of construction professionals to be licensed before carrying it out
- Each type of licenses has simple classes that indicate the complexity of work that professional is entitled to carry out

I submit that a licensing scheme establish a Code of Professional Conduct for AML/CFT Compliance Service Providers, similar to the recently introduced *Code of Professional Conduct for Financial Advice Services*.

I submit that the legislation establishes a Compliance Professional Services Committee to develop and administer the licensing regime and Code. In the short term, I submit that the regime relies on self-attestation and self-regulation by compliance service providers as is largely the case in the LBP scheme. Mechanisms for monitoring and enforcement of professional standards can be developed according to need.