GARY HUGHES
BARRISTER

[redacted]

Report to
THE COMMISSION OF INQUIRY INTO MONEY LAUNDERING IN BRITISH COLUMBIA, CANADA

For
THE HONOURABLE JUSTICE AUSTIN CULLEN

Regarding
THE ANTI-MONEY LAUNDERING REGIME OF NEW ZEALAND

Gary A. Hughes
Barrister
AKARANA CHAMBERS
Auckland, New Zealand

INTRODUCTION

I have been asked to provide a written report by way of evidence to the Commission that addresses New Zealand's legal and regulatory regime, and systems, that govern my country's anti-money laundering efforts. This report is intended to offer something of a comparative law view to the Commission, from another Western jurisdiction facing similar money laundering threats and challenges.

Included as part of the report are a range of comments upon the strengths and weaknesses of New Zealand's anti-money laundering ("AML") and countering financing of terrorism ("CFT") laws, and explanation of the range of captured New Zealand reporting entities, and the core legal obligations upon those entities. As well as that I add discussion of the related criminal proceeds recovery system, summarise recent high profile cases in the money laundering or anti-money laundering enforcement field, and address the data-sharing provisions for institutions engaged in AML/CFT related activities.

There is also a brief commentary on related legislative measures that aim to control foreign investment into, and corporate structures or tax trust structures enabling foreign involvement in, key New Zealand economic sectors. This reflects that, whilst an important plank of legal and economic policy, AML regulation should not be seen in isolation from other government policy measures intended to curb abuse of, say, the residential property market or taxation structures.

I have not been engaged in the work of the Commission to date, other than following some key milestones and developments via the Commission's public website. I have never worked in Canada or been admitted as a lawyer there. However, as part of background preparation for this report I have reviewed the following Canadian documents for context:

- Terms of Reference for the Commission of Inquiry;
- Interim Report of the Commission, November 2020;
- Dirty Money, independent review by Peter M. German QC, part 1, March 2018 and part 2, March 2019;
- FATF Mutual Evaluation Report on Canada, September 2016.

It crossed my mind in preparing this report, as it might for some Canadian readers, to wonder why British Columbia should be interested in learnings from a small remote jurisdiction like New Zealand? And how much the two societies and economies have in common, besides the obvious British Commonwealth colonial history and legal systems that are derived from the English common law model?

From a modest amount of factual research it can be suggested there are (even on a cursory look) some potentially relevant economic and legal points of comparison:

New Zealand and British Columbia

Basic comparative table of two Commonwealth economies

Feature	New Zealand	British Columbia
Population	5,112,300[1]	5,159,500[2]
GDP	321 billion (NZD)[3]	309 billion (CAD)[4]

[1] Stats NZ, Estimated Population, as at 30 December 2020 - https://www.stats.govt.nz/indicators/population-of-nz.

[2] Statistics Canada, British Columbia Population, as at 5 March 2021 - https://www.statcan.gc.ca/eng/subjects-start/population_and_demography.

[3] Stats NZ, Gross domestic product, as at 17 December 2020 - https://www.stats.govt.nz/topics/gross-domestic-product.

[4] Statista, Gross domestic product of British Columbia, as at 20 January 2021 - https://www.statista.com/statistics/577563/gdp-of-british-columbia-canada/.

Land mass	268,021 km²	944,735 km²
Largest city	Auckland, pop 1,571,718[5]	Vancouver, pop 2,606,351[6]
Government Structure	Single-chamber Parliamentary Democracy	Parliamentary Democracy
Electoral system	Mixed Member Proportional – 120 Members[7]	First Past The Post – 105 Senators[8]
Legal system	Common Law, derived from England, with major local statutory alterations	Common law, within a Federal/Provincial setting
Licenced Casinos	6[9]	19[10]
Registered Banks	27, incl 12 foreign[11]	35 domestic, plus 17 foreign (Federal, Canada)[12]
Practising Lawyers	14,039[13]	13,500[14]

The following 54 pages attached comprise my report, structured into 9 sections as follows:

1. Overview of New Zealand's legal regime for anti-money laundering, being the tripartite fields of criminal money laundering laws, anti-money laundering regulatory compliance controls, and a proceeds of crime confiscation system.
2. Description of the role of the branches of the New Zealand Police Financial Crime Group, and an evaluation of the strengths and weaknesses of each of them.
3. Analysis of the measures taken in New Zealand over the past decade to reduce money laundering, and evaluation of how effective those measures have been:
    a. measures taken (2009 to 2013) for financial institutions and casinos; and
    b. measures from 2016 onwards for designated non-financial businesses and professions.
4. Description of the different categories of reporting entities, and of the compliance and reporting requirements those entities face.
5. Description of how lawyers comply with their reporting obligations, especially in the face of competing obligations of solicitor-client privilege.
6. Description of the changes New Zealand has implemented over recent years to reduce overseas investment, of foreign control of companies and tax avoidance structures, along with comments on the linkages these measures might have had on money laundering activity.
7. Overview of the criminal proceeds recovery/restraint legislation and its processes.

---

[5] Stats NZ, Place Summaries, as at 2018 Census - https://www.stats.govt.nz/tools/2018-census-place-summaries/.

[6] World population review, Vancouver Population 2021, as at 5 March 2021 - https://worldpopulationreview.com/.

[7] New Zealand Parliament, Members of Parliament, as at 5 March 2021 - https://www.parliament.nz/en/mps-and-electorates/members-of-parliament/.

[8] Parliament of Canada, Senate of Canada, as at 5 March 2021 - https://sencanada.ca/en/senators/.

[9] Department of Internal Affairs, Gaming Expenditure Statistics 1984-2008, as at January 2008 - https://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats08.pdf/$file/Expendstats08.pdf.

[10] British Columbia, Casinos currently operating in B.C, as at 5 March 2021 - https://www2.gov.bc.ca/gov/content/sports-culture/gambling-fundraising/gambling-in-bc/gambling-locations.

[11] Reserve Bank of New Zealand register of registered banks and branches of overseas-incorporated banks, as at 18 May 2020 - https://www.rbnz.govt.nz/regulation-and-supervision/banks/register.

[12] Office of the Superintendent of Financial Institutions, Federal, website "Who We Regulate" page - https://www.osfi-bsif.gc.ca/Eng/wt-ow/Pages/wwr-er.aspx.

[13] NZ Law Society, *LawTalk* Issue 940, as at 1 May 2020. In total, 14,981 practising certificates had been issued, but 942 lawyers were based overseas.

[14] Information from the Law Society of British Columbia, as at 7 March 2021 - https://www.lawsociety.bc.ca/.

8. Summaries of a few high-profile New Zealand enforcement cases involving allegations of money laundering or anti-money laundering breaches.
9. Description of the data sharing provisions for reporting entities and third parties involved in AML compliance work, and their interaction our New Zealand privacy laws.

Thank you for this opportunity to contribute to the important work of the Commission.

Yours sincerely

Gary Hughes
Barrister
9 April 2021

1. OVERVIEW OF NEW ZEALAND'S LEGAL REGIME FOR ANTI-MONEY LAUNDERING

1.1. This part sets out a broad summary of the framework by which New Zealand currently seeks to detect and deter money laundering activity. That framework has advanced a considerable way in the past decade, through incremental but important changes, beyond the rudimentary anti-money laundering ("AML") law that was in place prior to 2009. This part also addresses, as context, that evolution of New Zealand's AML regime.

1.2. In my view, a holistic way to understand the AML regime is to characterise it as a tripartite system with three inter-dependent elements:

- The criminal laws that cover money laundering ("ML") definitions and offences;
- The regulatory system (part civil, part criminal) for anti-money laundering and countering the financing of terrorism ("AML/CFT") controls, which apply to private sector reporting entities; and
- The confiscation and forfeiture of assets under an active criminal proceeds recovery regime.

1.3. As will be apparent, the relationship between each element in the system is close and complimentary. Each element feeds into the next. The AML/CFT regulatory law forces banks, other financial sector firms, casinos, and related professionals and dealers in high value assets to monitor, detect and report money laundering behaviour. To do so, they first need to understand something of the money laundering criminal law, the second element – what it covers and why, what the relevant risks and criminal typologies may be, and how that applies to the risk areas in their own specific businesses by which criminals may misuse their services.

1.4. The third element (and key police objective) relies on output of that AML regulatory system, in the form of the reports of many kinds and provision of information onwards to the Police. An effective criminal proceeds/asset recovery system, which has probably been the most successful and visible part of the New Zealand system, feeds off those intelligence reports, a critical private sector input to the work of the Police financial intelligence unit, which in turn gathers and processes all the many suspicious reports or transaction reports filed under the AML regime and enables asset recovery operations as well as money laundering prosecutions.

1.5. It should be acknowledged that, like most national systems of money laundering control, the New Zealand laws inevitably twin the countering of terrorism financing with the countering of money laundering. That is consistent with the international norms and objectives of the global body, the Financial Action Task Force ("FATF"). However, recognising the scope of the Cullen Commission's Terms of Reference, and the primary concerns being money laundering, I do not address New Zealand's CFT rules specifically in this report.

International participation and pressures

1.6. The FATF was instigated by the G-7 nations in 1989. New Zealand has been a member of the FATF since 1991 and, as an early adopter and supporter, has had to date 4 of its public Mutual evaluations or reviews (plus a "follow-up" report). The effect is to provide an international peer review "name and shame" exercise, to pressure nations into improving their law or regulatory regimes, so as to deal with financial crime matters more effectively. Certainly, that process has had impact in this country. Early engagements with the FATF were what led to the arrival of a basic sort of AML law in New Zealand, the Financial Transactions Reporting Act 1996.

1.7. But financial complexity, time, and international expectations marched on. That 1996 statute was simple in its aspirations and very light in its fields of coverage and obligations upon the business community. By the time period after the 9/11 terrorist attacks in the United States, the FATF had been given a new mandate

and level of urgency, with global support in stepping up the so-called war on terrorism. The FATF issued new and expanded recommendations to counter terrorist financing and proliferation of weapons. And when working to produce its third Mutual Evaluation Report on New Zealand in 2008-9, the FATF identified a clear need to upgrade our older inadequate version of AML regulation so that it would move more in line with modern accepted international practice.

1.8. At a high level, the rules that were missing in the basic 1996 legislation included much more formal registration, regulatory oversight and clarity over which private businesses were subject to the AML regime, as well as detailed compliance obligations to ensure each captured business was forced to more deeply understand the activities of their customers, and focus on areas of its products/services that generate risk of money laundering.

1.9. The ultimate goal was to design a series of rules in a compliance framework designed to generate better, more frequent and systematic reporting of financial crime intelligence data to the Police, along with a regulatory framework to punish those entities that failed to meet the elevated compliance framework.

1.10. Meanwhile, adding fuel to the international peer pressure upon New Zealand, Australia had passed new federal legislation of this sort in 2006, in the shape of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Australian Commonwealth statute). New Zealand was becoming seen as a laggard that had not progressed beyond the basics of implementing FATF standards.

1.11. The spur to finally pass the new Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ("AML/CFT Act") was largely a response to that damaging mutual evaluation by FATF of New Zealand's legal regime. The FATF report was publicly released in October 2009, during the same week that final reading of the new AML/CFT Act was being passed into law in Parliament. Although that was a slightly choreographed effort to show the international community that moves were underway at the time, even if not yet implemented, the 2009 legislation represented a major step forward in addressing some of the legal and crime-fighting weaknesses found in the FATF report.

The Asia-Pacific Group on Money Laundering

1.12. FATF also operates alongside and through a number of "FATF-type" regional bodies around the world. New Zealand and Australia are active members of the Asia-Pacific Group on Money Laundering ("APG") which provides more localised support, guidance and capacity building around Pacific Island jurisdictions, based upon and mimicking the plenary frameworks and standards that the FATF espouses.

1.13. In practice that means for New Zealand officials there is often more regular, close international co-operation at the APG level than the plenary FATF body forum. This reflects the fact that AML efforts do rely on building neighbourly co-operation and mutual reciprocal processes with countries that are close in terms of trade, migration, diplomatic and economic connections.

1.14. At the time of writing, the FATF has carried out its latest mutual evaluation of New Zealand in 2020. It was delayed by Covid-19 issues but the evaluation report has now been completed – although not yet publicly released. That is likely to be made publicly available some time soon, in late April 2021.

AML/CFT regulatory bodies – the triple Supervisors model

1.15. As will be apparent, the NZ Police is the fulcrum to the whole AML system. In simplistic terms, receiving and synthesising private sector data so as to achieve actionable ML prosecutions and proceeds of crime recovery is the *raison d'etre* of the whole regime. But alongside the Police, a number of important actors help operate the increasingly complex regulatory regime.

1.16. There are 3 separate regulators of AML/CFT reporting entities, depending on the business sector they are in: the Reserve Bank of New Zealand ("RBNZ"), the Financial Markets Authority ("FMA"), and the

Department of Internal Affairs ("DIA"). The DIA also acts as default Supervisor for entities that do not squarely fit into one of the defined activities and sub-sectors.

1.17. The DIA is now the largest and most visible of the regulators, but all supervisory agencies work hard to ensure consistency across the regime. So, they tend to prefer to move in step on such issues as the drafting and publication of guidance or other material, which is done jointly as much as possible. This also applies to co-ordinating on enforcement priorities and initiatives. In the unlikely event that a particular Reporting Entity may potentially have two Supervisors, because of the different services it offers, the Supervisors will confer and determine which agency will take charge. Each Reporting Entity can have only one Supervisor.

1.18. Further, s 150 of the AML/CFT Act established an AML/CFT national co-ordination committee, due to the multiple agencies with an interest in this regime. Besides the 3 Supervisors this has as its usual members/representatives the:

- Ministry of Justice;
- New Zealand Police
- New Zealand Customs Service;
- Inland Revenue Department; and
- any other such persons as invited from time to time by the chief executive of the Ministry of Justice (e.g. government welfare/funding bodies such as the Ministry for Social Development and the Accident Compensation Corporate (ACC)).

1.19. Those agencies all talk to each other, meet regularly, and may share information when permitted under the AML regime, in the interests of law enforcement. As fulcrum, the NZ Police FIU/Commissioner in practical terms manages the information flows, while the Ministry manages the process and politics.

1.20. The DIA runs a separate peak-body industry consultation group with, for instance, the New Zealand Law Society (for barristers and solicitors), the Real Estate Institute of NZ (for real estate agents), and parties invited to participate occasionally as a person or trade association leading the interaction with a particular regulated sub-sector.

1.21. More detail on these regulators and their powers is provided in Part 4 of this Report below.

Predicate offences and criminal money laundering offences

1.22. The formal statutory money laundering offences are found in s 243 of the Crimes Act 1961, with maximum penalties of potentially up to 7 years in jail for those convicted.

1.23. The offence provisions refer to a "person" engaging in a money laundering transaction (section 243(4)). The Crimes Act defines a person as including any public body or local authority and any board, society or company in relation to acts that it is capable of doing so. Therefore, both legal and natural persons can be prosecuted for money laundering. Although the penalty for money laundering is a term of imprisonment, under the Sentencing Act 2002 a court may impose a fine instead, as it inevitably has to in the case of a legal entity. The requisite knowledge and intention to commit the offence can be imputed to a body corporate through its human agents. In practice, most cases in the past have been taken against individuals.

1.24. The key elements of a "money laundering transaction", paraphrased from s 243(2)–(4), involve a person:

- dealing with, or assisting in dealing with, any property for the purpose of concealing it or enabling another person to conceal any property; and
- knowing or believing that such property is the proceeds of a criminal offence, or being reckless as to whether it is the proceeds of offending.

1.25. "Property" is widely defined as including real and personal property of any description whether situated in New Zealand or elsewhere and whether tangible and intangible and includes an interest in any such property. "Conceal" is defined as concealing or disguising the property and includes (without limitation) converting the property into another form and concealing or disguising the nature, source, location, disposition, or ownership of the property or of any interest in the property. "Deal with" means to deal with the property in any manner and by any means and includes (without limitation) disposal, transferring possession or bringing the property into or removing it from New Zealand.

1.26. The *mens rea* or state of mind required for money laundering is a knowledge or belief that all or part of the property is the proceeds of an offence, or being reckless as to whether the property is the proceeds of such an offence. Part of the package of definitions (in s 243(1)) means knowledge must also include some intention to conceal the property or to assist another to do so.

1.27. There is also a lesser offence of possession of property for money laundering purposes, punishable by up to 5 years in jail rather than 7 years. In order to establish this offence, it must be proven that the property was the proceeds of an offence committed by another, and that the accused had the requisite knowledge or was reckless, *and* intended to engage in a money laundering transaction in respect of that property (section 243(3)).

1.28. There is no monetary threshold or other limitation on the types of assets or transactions for prosecution under section 243 of the Crimes Act – so if it were a *de minimis* level of transaction that affects only prosecutorial discretion on whether a case is worth taking, rather than legal responsibility.

1.29. The underlying criminal behaviour is called the predicate offence. For Crimes Act purposes, this means any crime can in effect form the basis of a separate money laundering offence. The ML offence is a secondary but often broader offence, one that relates to dealing with the proceeds or property of that crime. The relevant predicate offence can be virtually anything – it is defined very broadly to mean any offence (or any offence described as a crime) "that is punishable under New Zealand law, including any act, wherever committed, that would be an offence in New Zealand if committed in New Zealand." Up to 2015, it was defined in terms of only serious offences, deemed to be those punishable by a term of imprisonment of 5 years or more, but that limitation was removed.

1.30. Although it is helpful for regulated reporting entities to get to know the signs and how to spot types of predicate crime, they are not expected to precisely identify which offence they suspect is involved. When reporting to Police there are a set of potential indicators that they can choose or nominate. But just as a reporting entity may not be sure what offence is in issue, merely that something has aroused suspicion, even a prosecutor under s 243 of the Crimes Act does not have to prove any intent to conceal the particular property/assets/funds, or that they were the proceeds of any particular predicate offence.

1.31. In a prosecution, it is also no defence for the owner to say Police have pleaded the wrong predicate offence (implying there may be some different type of offending not identified in the charges actually laid).

1.32. An important further extension to the criminal law, given the interconnectedness of global commerce, is that there is an element of extra-territoriality. Any action taken outside of New Zealand that would have been an offence under the equivalent New Zealand law, if done here, is also a money laundering offence under s 245 of the Crimes Act.

1.33. There were previously specific drug-money laundering offences set out in s 12B of the Misuse of Drugs Act 1975, removed in 2015. The policy is now to broadly capture any offence, including drugs offences, as being covered by s 243, rather than singling anything out in specific offence provisions (apart from

separate terrorism crimes contained in the Terrorism Suppression Act 2002). In practice, organised drug crime remains the top target of the Police groups involved.

1.34. There is also a codified defence under section 244, if the accused can prove that the act or step to which the charge relates was done by them in good faith for the purpose of, or in connection with, the enforcement or intended enforcement of:

- these s 243 money laundering provisions;
- the Criminal Proceeds (Recovery) Act 2009;
- the AML/CFT Act 2009; or
- the Financial Transactions Reporting Act.

1.35. That would typically relate to directions from the Police on how to deal with funds or with customers after a suspicious report has been made, such as a bank being instructed to keep an account open even while under suspicion.

Criminal proceeds/assets recovery

1.36. The AML/CFT Act is best understood alongside its counterpart legislation, passed at the same time during the one Parliamentary term in 2009, the Criminal Proceeds (Recovery) Act 2009 ("CPR Act"). The CPR Act sets out a detailed legislative scheme relating to obtaining court orders that will freeze and then ultimately confiscate the proceeds of crime.

1.37. Unlike the previous forfeiture law, a criminal conviction is not required for the imposition of a forfeiture order — all that is required is proof of "significant criminal activity" on the balance of probabilities.

1.38. The CPR Act has become a very powerful and well-used tool in the hands of New Zealand asset recovery units. Critical information that drives it, which enables the freezing and seizing of ill-gotten gains from fraudsters, drug dealers and criminals, is provided by reporting entities under the AML/CFT Act. Those two pieces of legislation are best seen as two sides of the same coin, or as key components of a machine developed specifically to identify, report, and then strip away the profits of crime.

1.39. The CPR Act restraining system has grown into probably the most successful and visible element of our regime, with resulting inroads into criminal fortunes being made in the decade or so that New Zealand's modern AML/CFT laws have been in place.

1.40. More detail on this regime is provided in Part 6 of this Report below.

2. ROLE OF DIFFERENT PARTS OF THE FINANCIAL CRIME GROUP WITHIN NEW ZEALAND POLICE

2.1. A core part of the AML/CFT regime is of course the voluminous work dissecting and processing the thousands of reports made by reporting entities. For that reason, the New Zealand Police Financial Intelligence Unit ("FIU") is a vital agency in the regime, equivalent to FinTRAC in Canada.

2.2. The FIU is a part of the wider Police Financial Crime Group ("FCG"), which now has three arms to it. The FCG is made up of the Financial Intelligence Unit, a total of 5 Asset Recovery Units, a Money Laundering Team, and a headquarters group based in Wellington.

2.3. Many of the statutory obligations are generalised upon the office of the Commissioner of Police, but in practice this means the Financial Intelligence Unit. That unit has formal obligations under section 142(b)(i) and section 143(b) of the AML/CFT Act 2009 to produce educational and guidance material, and takes to that task strongly and professionally, including by increasing use of social media channels to get messaging across to the public.

2.4. Compared to the FIU structure of our nearest neighbour country, Australia, a key difference is that the New Zealand FIU sits firmly within the Police structure, and is not bundled in alongside the AML/CFT regulatory Supervisor functions, as is the case with AUSTRAC in Australia. I consider that to be an overall strength in our institutional structure, as it enables deep and rapid integration of the intelligence gathering/suspicious reporting function with a range of active Police operational teams.

Financial Intelligence Unit

2.5. The Financial Intelligence Unit has been operational since 1996. Its core function is to receive, collate, analyse and disseminate information contained in Suspicious Activity Reports (SAR), Prescribed Transaction Reports (PTR), and Border Cash Reports that various persons are obliged to make under the AML/CFT Act. It develops and produces a number of financial intelligence products, training packages and policy advice.

2.6. The FIU participates formally in the AML/CFT National Coordination Committee chaired by the Ministry of Justice, and chairs the Financial Crime Prevention Network (FCPN), which is explained in more detail in part 9 of this report.

2.7. The FIU is an active contributing member to international bodies such as the Egmont Group of Financial Intelligence Units and the Asia/Pacific Group on Money Laundering, as well as key FATF multilateral initiatives. New Zealand's FIU is an active contributor and collaborator on cross-border mutual criminal investigation matters: through the Egmont Group, FIU figures suggest that in the period 2016 - 2019 it responded to over 380 requests for assistance from foreign countries and sent more than 180 requests itself. During this same period, approximately 500 intelligence reports were shared with international partners.

2.8. The FIU provides a number of training and educational outreach events, including a major annual conference held in Wellington, and also produces a monthly report on some of its past operations and statistics. These reports and case studies are based upon FIU materials (when they become publicly accessible, or after a court case had concluded) and also open source media reporting collected from around the globe on money laundering matters of interest, and provided to reporting entities to help educate and keep them up to date.

2.9. The FIU grew considerably in prominence after the AML/CFT Act became law in October 2009, from a small and rather insular part of the broad Police organisation. As a result of new staffing, financial resourcing and analytical tools investment, it now plays a more public role to assist in detecting and deterring money

laundering, and contributing to public education and awareness of flaws in the financial system that allows criminal enterprise to keep making profits.

Asset Recovery Units

2.10. The New Zealand Police Asset Recovery Unit ("ARU") was first established in December 2009 specifically to implement the Criminal Proceeds (Recovery) Act 2009 and take advantage of its non-conviction based, balance of probabilities only, weapons for early and surprise operations against criminal assets.

2.11. The ARU is in effect a turbo-charged successor to the previous Proceeds of Crime Unit, which were established in 1991, and later combined with the FIU to create the Financial Crime Group.

2.12. The CPRA expanded the regime for the forfeiture of property that has been directly or indirectly acquired or derived from significant criminal behaviour. It is intended to reduce the possibilities for individuals or groups to profit from criminal behaviour, to reduce the opportunities they have to expand their criminal enterprises, and act as a deterrent for criminal activity.

2.13. From one unit in 2009, there are 5 ARUs now, based in regional centres at Whangarei, Auckland, Waikato/Bay of Plenty, Wellington, and Christchurch. They deploy regularly on high profile asset seizure operations, usually driven by FIU intelligence work and evidence, which in turn often derives from key Suspicious Activity Reports assembled from a rich vein of information reported by banks and various AML/CFT reporting entities.

Money Laundering Team

2.14. The Money Laundering Team ("MLT") is the newest element of the Police FCG. It was not part of the initial two arms, being just the intelligence gathering and processing arm, and the regional asset recovery operations hitting criminals on the ground. However after the increasing success of prosecutions for anti-money laundering criminal matters and, perhaps, a growing realisation that in many case the elements of proving a money laundering charge may in practice be easier than proving an underlying predicate offence (e.g. fraud charges), this specialist team was established in 2017.

2.15. Its intended job is to target money laundering risks more specifically, centralise evidence gathering and prosecution materials for a money laundering case. That can help reduce the investigative gap sometimes found in disparate teams of police detectives workings on matters around the country and handling financial investigations into complex crime. A related unit, known as OFCANZ in the past and now NOCG (see below) has a specialist focus on motorcycle gang activity and other organised criminal groups.

2.16. The MLT investigate criminal offenders moving the proceeds of predicate offending. The focus of the team is on disrupting and dismantling facilitators assisting organised criminal groups to hide illicit funds, including complicit Designated Non-Financial Business and Professions and other third parties such as money remitters.

The National Organised Crime Group (NOCG)

2.17. Outside of the FCG sits the National Organised Crime Group ("NOCG"), another New Zealand Police organisational group that has an extensive multi-agency focus.[15] NOCG centralises and enhances intelligence gathering against organised crime groups, including those committing financial crime, so information is shared between law enforcement and other relevant agencies. Staff within the NOCG collaborate with, and enhance cooperation between, law enforcement and other relevant agencies in planning and conducting operations, both nationally and internationally.

[15] National Organised Crime Group, https://www.police.govt.nz/careers/police-groups/national-organised-crime-group.

2.18. The NOCG was established from 2017 to replace a forerunner unit known as the Organised & Financial Crime Agency of New Zealand (OFCANZ). NOCG is responsible for:

> "intelligence gathering, analysis and dissemination, including information sharing, strategy and priority setting, target setting and planning, undertaking, and supporting investigations using overt and covert capability, focus on preventing crime and reducing social harm, maintaining international linkages, and strategic liaison with relevant agencies in New Zealand, transnational, and national level operational targeting of organised crime groups."[16]

2.19. The ultimate stated goal for this unit targeting organised crime gangs is for New Zealand to become an even safer country, with a strong reputation as a safe place for other countries to deal with and a reduction in social harm in our communities. That might be broadly the same summary for the overall combined objectives of these various agencies and units within the NZ Police.

[16] New Zealand Government, Policy Briefing to the Incoming Minister of Police, as at November 2020 at B-9. https://www.beehive.govt.nz/sites/default/files/2020-12/Police%20-%20Part%20B.pdf.

3. THE ANTI-MONEY LAUNDERING REGULATORY REGIME

3.1. Parts 3 and 4 of this report provide a detailed analysis of the measures taken in New Zealand over the past decade to reduce money laundering. Although the regime is still in reality in its infancy, I offer some tentative evaluation of how effective those measures have been and the strong and weak areas in the regime, and describe some of the AML measures/obligations in terms of the 3 Supervisors and how they regulate and use enforcement powers to control the reporting entities they are responsible for.

3.2. The AML/CFT Act contains a helpful, expansive purpose statement, which is always valuable to bear in mind. When it comes to resolving ambiguities or interpretative difficulties (of which, it must be said, this statute has more than its fair share!) it is one of the key guiding provisions a Judge will refer to:

> Section 3 Purpose Statement of the AML/CFT Act
>
> (1) The purposes of this Act are—
>
> (a) to detect and deter money laundering and the financing of terrorism; and
>
> (b) to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and
>
> (c) to contribute to public confidence in the financial system.
>
> (2) Accordingly, this Act facilitates co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies.

3.3. Analysis of New Zealand's AML rules is most conveniently split into a description of two key phases, being:

- measures taken (2009 to 2013) for financial institutions and casinos (Phase 1); and
- measures from 2016 onwards for designated non-financial businesses and professions (Phase 2).

Phase 1 measures to deal with financial institutions and casinos

3.4. As explained in part 1 of this report, the AML laws moved through a period of major transition in the period 2008-2013, designed to greatly enhance New Zealand's degree of compliance with the FATF's 40 Recommendations (then, the October 2004 version of those Recommendations).[17]

3.5. The philosophy of the AML/CFT Act when passed was to fully embrace the FATF "risk-based approach", meaning that it largely eschews prescriptive detail in the language of the Act itself, and applies broad and flexible statutory tests inviting firms to decide for themselves how to meet those tests, on a risk-based framework. It is principles-based legislation, in some aspects simply adopting verbatim the flexible FATF wording of a particular standard or recommendation, leaving much of the detail still to be elaborated upon in subsidiary documents and guidance found elsewhere.

3.6. The new law had a long gestation period, as the relevant government ministries first began public consultation on reforms as far back as 2005, and then when it was finally passed an equally long implementation period, as it only came into full force and effect from 30 June 2013.

3.7. Since the AML/CFT Act contains only the key principles and umbrella provisions, significant matters of detail are instead addressed in the Regulations and Codes and Gazette notices intended to be made under it. Equally, there remain a lot of grey areas of interpretation and, since the regime in only still in its infancy,

[17] FATF Standards, FATF 40 Recommendations, October 2003, (incorporating all subsequent amendments until October 2004), since superseded in 2012, but available at: http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

not much authoritative case-law guidance yet. That has permitted the Supervisors an exceptionally wide discretion as regulators in how they each choose to interpret the many grey areas – not always an ideal regulatory outcome or leading to a level-playing field.

3.8. The 3 Supervisors have to date agreed and issued only one Code of Practice - for Identity Verification CDD purposes (first in 2013, since amended). It is to be hoped more Codes can be promoted over time, as they are a useful compliance tool. That is because, although not mandatory, if complied with a Code provides a form of safe harbour to institutions who fully comply with its terms and follow its suggestions, as they are deemed to in compliance on that aspect of the statutory obligation, unless specifically proven otherwise.[18]

3.9. With a long implementation period planned, a bare statutory framework at principles level only, and regulators themselves still getting up to speed, reporting entries could be forgiven for concentrating their scarce compliance resources elsewhere until 2013. Even then, many small businesses struggled with the details of early application of Customer Due Diligence ("CDD") and other rules, while large banks with deep resources and overseas owner experience were taking big compliance strides forward.

3.10. At a high level, some of the primary legal obligations in the AML/CFT Act require affected entities to:

a. Carry out a risk assessment on current and potential customers, products/services and business partners.

b. Establish, implement, maintain and regularly audit a set of AML/CFT compliance policies and procedures (known as a "compliance programme".

c. Appoint a person to act as an AML/CFT compliance officer to administer the compliance programme.

d. Set up processes to vet new senior managers and staff engaged in AML/CFT related duties (Including the compliance officer) and to train those persons on AML/CFT risks and related compliance matters.

e. Ensure there are governance structures to keep senior management and directors of companies involved, so the compliance officer and compliance function is not left in a silo.

f. Comply with more rigorous CDD requirements, including determining when Enhanced CDD is required, and when Simplified CDD might be permitted.

g. Regularly monitor customer activity (accounts and transactions), especially in relation to certain high-risk transactions or types of business relationships.

h. Ensure a robust process exists to detect and then report suspicious activities, and other prescribed types of transactions, to meet systematic reporting requirements to the Police FIU.

i. Maintain full record keeping for 5 years after the end of a transaction or customer relationship;

j. Carry out ongoing review, independent auditing and annual reporting about the entity's compliance with its AML/CFT compliance programme.

3.11. This section below next covers a selection of four key foundational steps a reporting entity must take. I then return to other detailed compliance aspects listed, later, in part 4 of this report.

Each entity must have a person acting as AML/CFT Compliance Officer

3.12. One of the core legal obligations on every Reporting Entity is to appoint a person to act as its AML/CFT Compliance Officer ("AMLCO"). But despite the pivotal role this person will play in making each firm's AML/CFT Programme successful, the legislation and even the available guidance material is surprisingly sparse on what expectations and workstreams the role entails.

56 Reporting entity must have AML/CFT programme and AML/CFT compliance officer

[18] See s 67 of the AML/CFT Act – legal effect of codes of practice. Anti-Money Laundering and Countering Financing of Terrorism Act 2009 No 35 (as at 15 March 2021), Public Act Contents – New Zealand Legislation.

> (1) A reporting entity must establish, implement, and maintain a compliance programme (an **AML/CFT programme**) that includes internal procedures, policies, and controls to—
>
> (a) detect money laundering and the financing of terrorism; and
>
> (b) manage and mitigate the risk of money laundering and financing of terrorism.
>
> (2) A reporting entity must designate an employee as an AML/CFT compliance officer to administer and maintain its AML/CFT programme.
>
> (3) In the case of a reporting entity that does not have employees, the reporting entity must appoint a person to act as its AML/CFT compliance officer.
>
> (4) The AML/CFT compliance officer must report to a senior manager of the reporting entity.
>
> (5) …[*omitted*]

3.13. Therefore, much of the scoping of an AMLCO's role is left to be developed by the regulators and auditors as "good practice" or by building industry experience over time. Together with a huge variation amongst reporting entities in size, resources, and level of education/training, there is a wide discrepancy in levels of understanding and hence performance of AMLCOs across the covered market.

3.14. A large institution may have teams of specialists in finance crime and regulation, each focused deeply on specific areas, such as ECDD or Monitoring, or Economic Sanctions. But in a great many small businesses it is not uncommon to find the same person tasked with being the AMLCO has to wear various other legal or commercial hats – such as Health & Safety officer, Privacy officer, or accounting or administrative roles as well. The level of time and energy that can be devoted to AML/CFT issues in small-medium enterprise businesses is usually very constrained.

3.15. Despite those challenges, the requirement to force each entity to appoint an individual with responsibility for managing its AML Programme is a strength of the system. It ensures each covered business large or small has a person inside it with accountability and incentive to press others in the team into compliance.

Entities must ensure Senior Management reporting and governance

3.16. A set of related important legal obligations include that regular reporting lines exist from the AMLCO to senior management. This is meant to signify that the AMLCO role cannot be fobbed off to a junior staff member and must report to directors or senior managers, a group of persons in the firm who also be trained specifically in AML/CFT relevant issues.

3.17. A senior manager is considered person in the business who occupies a position as or equivalent to a director, or in a law firm such role as partner or trustee, or any other person in a position to influence the management or administration of the business (akin to a "shadow director" concept in company law). It is possible to be both the senior manager and the AMLCO all at one time, although most businesses of a reasonably size will try to employ somebody with specialist compliance skills given the increasingly demanding nature of that role.

3.18. Section 56(4) of the AML/CFT Act requires the AMLCO to report to a senior manager (if that person is not already themself at senior management level). The purpose of this requirement is to show that the owners and governance individuals of a reporting entity are still in charge and on the hook for AML compliance. They cannot delegate away those responsibilities to an employee.

3.19. Guidance issued by Supervisors to Reporting Entities emphasises the importance of governance structures around AML/CFT, and the need for management to take an interest. They need to take responsibility for ensuring problems, red flag alerts, customer termination decisions and similar issues reported up the chain by the AMLCO, are all must addressed and appropriate decision-making happens in a timely way, and records are kept. The Board as a governance priority should also ensure that the person appointed as the AMLCO has sufficient expertise, access to training, and influence over business information and systems in

order to properly discharge their duties, as well as the authority and confidence to advise senior management on AML matters requiring their attention.

3.20. The way in which this reporting function happens is not specified — but it should be documented in the compliance programme, as auditors and the Supervisor will want to test how well it is working. Also, the entity needs to keep regular records of how and when senior management reporting operates. Nothing is prescribed, but best practice suggests regular documented reports and meetings on a business-as-usual basis are necessary, along with clear and simple procedures to escalate more urgently when required.

3.21. Usually, the Board will review and sign off on the AMLCO's preparation of the two major written materials that will guide the rest of the AML/CFT compliance work – being a written risk assessment of money laundering risk, and a document or documents package making up the compliance programme of procedures, policies and controls.

Prepare a detailed Risk Assessment document, evaluating money laundering risks

3.22. The first and probably more important of those two substantive written pieces of work is the risk assessment. Unlike some other jurisdictions, New Zealand requires a standalone written risk assessment to be prepared, as a first step and key platform for all the AML/CFT compliance steps to follow.

3.23. Outside the main commercial banking sector, the New Zealand financial landscape involves a wide variety of reporting entities, large and small, with diverse risk profiles and compliance resources available. The law requires each financial business to develop risk-based systems and controls that are appropriate for its own nature, size and complexity of the business and the money laundering (ML) and terrorist financing (TF) risks it may face.

3.24. The Risk Assessment is essentially a business due diligence report, focused upon each individual business, that must be tailored to the type of risks each business is likely to face in its own unique sphere of operations. In particular, this must be completed before entering a new client relationship or onboarding new customers for captured services (i.e. conducting Client Due Diligence on new customers). Completing a risk assessment means, more precisely, a reporting entity must examine and document "the risk of money laundering and the financing of terrorism that it may reasonably expect to face in the course of its business."[19]

3.25. The Risk Assessment cannot be done once, then left on the shelf. There are statutory requirements for it to be reviewed and updated regularly, and kept available for the AML Supervisor's staff (and the firm's external auditor) when they wish to inspect or when the biennial independent audit is due.

3.26. Section 58 of the AML/CFT Act details the specific legal requirements of the risk assessment, as follows:

> (1) Before conducting customer due diligence or establishing an AML/CFT programme, a reporting entity must first undertake an assessment of the risk of money laundering and the financing of terrorism (a **risk assessment**) that it may reasonably expect to face in the course of its business.
>
> (2) In assessing the risk, the reporting entity must have regard to the following:
>
> (a) the nature, size, and complexity of its business; and
>
> (b) the products and services it offers; and
>
> (c) the methods by which it delivers products and services to its customers; and
>
> (d) the types of customers it deals with; and
>
> (e) the countries it deals with; and

[19] See s 58(1) of the AML/CFT Act.

(f) the institutions it deals with; and

(g) any applicable guidance material produced by AML/CFT supervisors or the Commissioner relating to risk assessments; and

(h) any other factors that may be provided for in regulations.

(3) The risk assessment must be in writing and—

(a) identify the risks faced by the reporting entity in the course of its business; and

(b) describe how the reporting entity will ensure that the assessment remains current; and

(c) enable the reporting entity to determine the level of risk involved in relation to relevant obligations under this Act and regulations.

3.27. The point of this detailed risk assessment exercise is to evaluate all the criminality risks that the particular firm may reasonably expect to face in providing whatever special services it delivers, to its own unique customer base. But s 58(3) of the AML/CFT Act elaborates more directly on the other purpose of the Risk Assessment – to evaluate in sufficient detail the ML and TF risks faced by the entity, so that it can properly determine the level of risk involved in scenarios that will arise later when carrying out other relevant AML/CFT obligations contained in the Act or Regulations.

3.28. Many jurisdictions around the world require a form of risk assessment, or a set of assumptions that it will be done as part and parcel of overall KYC steps when taking on new customers or opening up new product lines. Nothing ground-breaking arises in expecting regular risk-assessments. However, in my view a key strength of the New Zealand approach is that by requiring it as a first, stand-alone written report, before the reporting entity confirms other parts of its compliance programme, entities are forced to pay attention to the actual underlying ML risks in their particular field of activity. That provides a stronger linkage to and understanding of the point of the AML regulatory work – the criminal money laundering threat itself. Otherwise, the underlying financial crime elements can get lost in a mass of tick-box compliance documents and procedure manuals. That can still happen in New Zealand entities but, if done well, a document-preparation process devoted to evaluating the risks of ML in the business helps avoid that.

Annual reporting to the Supervisor, and two-yearly independent audit processes

3.29. Reporting entities are required to produce to their AML/CFT Supervisor an Annual Report, covering their business captured activities and information about the current state of their Risk Assessment and Compliance Programme. Additionally, Each reporting entity must submit its AML/CFT materials to external independent audit every 2 years (in forthcoming Regulations later in 2021 this may be extended to every 3 years), or sooner at other time if requested by their Supervisor (see AML/CFT Act, ss 59 -60).

3.30. Together, these two milestone provisions create a scenario where entities know that an external pair of eyes will be reviewing their compliance efforts regularly, and this builds incentives to make proper efforts and not let the compliance programme simply gather dust.

3.31. In legal requirement terms, the Annual Report to the Supervisor will be one that:

- follows a prescribed form (which may change from year to year as determined by the Supervisor);
- takes into account the results and implications of the external audit required by s 59(2) of the Act;
- may contains other information if prescribed by Regulations from time to time, so it can be responsive to changing circumstances or financial crime threats; and
- has to be provided at a time to be appointed by the Supervisor each year, completed via an online upload system, and usually prepared by or under oversight of the AMLCO.

3.32. Reporting entities also have a separate legal obligation under s 59 of the AML/CFT Act to regularly review their AML/CFT written materials, and confirm in their Annual Reports to the Supervisor that they have done so. Again, this is a powerful reminder that the compliance materials are meant to be living

documents, refreshed often. No timeframe is specifically prescribed, so entities are free to apply their own views on the frequency and intensity of review, but the purpose of these reviews as stated in the Act is in order to:

- ensure that those documents are still up to date and current;
- identify any deficiencies in the effectiveness of the Risk Assessment and Compliance Programme;
- make any changes to the Risk Assessment and Compliance Programme identified as being necessary.

3.33. For the independent audit process, a more intrusive external set of checks, s 59B of the AML/CFT Act gives more detail on appointing an auditor who will be in a position to do an independent review, and be appropriately qualified to conduct the audit. The independent audit should assess, amongst other things:

- whether the Risk Assessment meets the requirements of s 58(3) of the AML/CFT Act (i.e. the auditor does not seek to second guess the level of risk ratings actually ascribed by the business to its functions);
- the effectiveness of the Compliance Programme measures having regard to the firm's own assessed ML/FT risk (a process of testing whether policies, procedures, and controls appear to be working in practice in the entity);
- the extent of compliance with the AML/CFT Act, Guidance Notes, Codes of Practice and Regulations as they apply to the firm.
- whether the Compliance Programme has been effectively implemented, or changes are needed;
- whether the firm has complied with its stated Compliance Programme in all material respects.

3.34. The auditor may wish to work remotely by receipt of documents (especially since Covid-19), or, preferably, to spend time visiting on site to examine individual client/matter/transaction files at random, and wanting to locate records to see that KYC requirements have been understood by staff and correctly applied. That process will usually involve dialogue with the firm's AMLCO to test understanding and effectiveness of the firm's compliance systems. If an experienced auditor is involved, it enables the AMLCO to get an informal sense of benchmarking against what the auditor sees as best practice levels of compliance across a sector.

3.35. One notable market failure in this area has been a shortage of skilled AML auditors to fulfil this independent function. That has been exacerbated by the Phase 2 additions of a great many more reporting entities to the AML net, without corresponding number of reliable auditors yet available. This is expected to ease over time, but is causing angst in some areas where new or unskilled persons are entering the market as auditors, a field where there is little defined pre-requisite or skill-set minima, beyond the statutory language in s 59B of the Act. That bare provision simply says the person must be "appropriately qualified to conduct the audit" and is not required to be a chartered accountant or qualified to undertake financial audits. A regulatory audit requires quite a different skill-set.

3.36. On the whole, however, in my view the internal review, external audit, and annual report measures are a useful and successful discipline to ensure entities keep AML/CFT compliance current and front of mind.

Phase 2 measures to bring the non-financial professions under AML/CFT coverage

3.37. A wider 'Phase 2' coverage of Designated Non-Financial Businesses and Professions ("DNFBP") was originally contemplated at the outset when the Ministry of Justice was framing the AML/CFT Exposure Draft Bill in 2008. But lawyers and other DNFBPs lobbied vigorously and successfully, not to be caught in the new AML/CFT Act at the time it was passed in 2009. Political complexity meant it sat on the drawing board when all financial sector entities were captured from mid-2013. But that did not mean concerns about professionals and advisors, sometimes described as "gatekeepers" because they help others access the financial and legal system, had gone away.

3.38. Similar concerns existed about brokers/dealers in luxury vehicles, boats, jewellery or assets that are highly liquid/transportable and therefore provide a good rapid way of trading in the proceeds of crime for something more tangible and harder to trace. They were also newly brought under the AML regime, to a more limited extent, from the 2017 Amendment reforms.

3.39. When lawyers and accountants were outside the captured net of reporting entities after 2013, anomalies started to appear, and concerns remained about lawyers being involved (knowingly or otherwise) in money laundering. The Police FIU believed that lawyers under-report suspicious transactions, and may be unwittingly complicit in more laundering activities than they realise. Then the Panama Papers highlighted risks in legal services for trusts and opaque corporate structures, as did publicity around how banks were handling the new Phase 1 law and the customer friction it was initially creating. But, despite all the new awareness and publicity around the 2009 Act, the average level of reports by lawyers to the FIU actually dropped, from 9.7 to only 7 per year. For captured Phase 1 financial entities, according to the FIU, reporting in the first couple of years after implementation increased by over 350%.

3.40. Phase 2 reforms were really only accelerated as a political reaction to the embarrassment of the Panama Papers disclosures - with New Zealand in danger of becoming branded as a tax haven alongside Belize, the Seychelles, and other sunnier places. As a result, lawyers were the first professional sector of the DNFBP categories to be captured by the AML regime. But ML risks also affect licenced conveyancers, accountants, real estate agents, and selected dealers in high-value assets (e.g. luxury items, cars, boats, jewellery, precious metals and stones, artefacts and artwork). All have been transitioned into the system over the last 2.5 years and now co-exist as reporting entities alongside banks, casinos and financial system players.

3.41. Comparatively, the Australian government continues to resist introducing its own "Tranche 2" coverage for lawyers. Lobbying against the extra compliance cost remains strong, although public and media pressure appears to be building.

3.42. The specific catalyst to bring forward the New Zealand changes was the Shewan Report of 2016, responding to the *Government Inquiry into Foreign Trust Disclosure Rules.*[20] That final report recommended the AML/CFT change, in these terms:[21]

> Expansion of scope and application of AML rules
>
> 12.15 For services provided to foreign trusts, consideration be given to the removal by Order in Council in the short term (prior to 31 December 2016) of the regulation that excludes lawyers and accountants from AML reporting requirements. The proposed removal of this exclusion when phase 2 of the AML regime is implemented, as announced by the Government in May 2016, will address this recommendation but may not be effective until towards the end of 2017 or later.
>
> 12.16 The AML legislation or regulations be revised to include a mandatory requirement to verify in all cases the underlying source of funds or wealth settled on a foreign trust.
>
> 12.17 Expanded guidelines be issued explaining the scope of customer due diligence required in establishing and verifying beneficial ownership, effective control and source of funds in complex multi-layered trust structures. These should include a series of detailed worked examples.
>
> Suspicious transaction reporting
>
> 12.18 The legislation or regulations that govern suspicious transaction reporting to FIU be revised to facilitate the reporting of actual or proposed transactions that have not or will not necessarily go through a New Zealand bank.
>
> 12.19 Greater profile, coupled with training recommendations, be given to the obligation on trust service providers to report suspicious transactions.

[20] Report of the Government Inquiry into Foreign Trust Disclosure Rules, John Shewan, 27 June 2016, available at: https://www.treasury.govt.nz/publications/information-release/government-inquiry-foreign-trust-disclosure-rules

[21] Shewan Report, above, at p 53-54. Other recommendations focused on tightening registration process for foreign trusts, disclosure and data-flows to Inland Revenue, ongoing tax filing details, fees and obligations, some feeding into FATCA or CRS inter-governmental process.

Information sharing

12.20 A review be undertaken of the current legislative arrangements for the sharing of information between the three agencies (IRD, FIU and DIA) with supervisory responsibility for disclosures by foreign trusts (and other entities). The purpose of the review, which could coincide with the introduction of phase 2 of the AML regime, would be to determine the financial and efficiency gains and other implications (including secrecy considerations) of sharing strategic intelligence and other information between agencies.

3.43. The 2017 Amendment Bill also made some important changes for all reporting entities, not just the new Phase 2 sectors. A key reform was introducing Prescribed Transaction Reports ("PTR") – mandatory regular transaction reporting obligations, regardless of whether there has been anything suspicious or not. All businesses covered by the AML/CFT Act now have to report international wire transfers and physical cash transactions over certain amounts (hence the prescribed thresholds for transactions) to the FIU. The purpose of this new series of reports was to provide data transparency that will make it more difficult for criminals to employ multiple small transactions, multiple senders or multiple recipients as methods to avoid detection. Phase 1 business were eased into this new process from 1 November 2017 onwards; Phase 2 firms must report prescribed transactions from the date they became covered by the Act.

3.44. Prescribed transactions are defined in s 48A-C of the Act, with dollar thresholds set by Regulations as:

- international wire transfers of NZ$1,000 or more;
- physical cash transactions of NZ$10,000 or more.

3.45. Reporting entities therefore have several contact points with the different AML agencies, especially their sector Supervisor but also including the Police FIU. These include having to be registered with the Police FIU (for login access to its online reporting portal), then occasionally making a report of suspicious matters (known as a Suspicious Transaction Report up to 2017, and as a Suspicious Activity Report or "SAR" since) and also making regular PTRs for large cash or international wire transactions. Any of those points of contact could result in a request for further information/investigation from the FIU, or potentially some dialogue back-channelled from the FIU to the relevant Supervisor about the entity's perceived issues.

3.46. In a significantly reduced burden for high value asset dealers, the SAR rules are voluntary, not mandatory for them – if a customer's activity is suspicious, say in purchasing a car or boat, they may decide to file a SAR with the FIU, though this is optional. But instead the PTR process is made more central for high value dealers: they must file prescribed transaction reports to the FIU on cash transactions of $10,000 or more.

The AML/CFT Supervisors' functions, powers and enforcement approaches

3.47. Before briefly considering the powers and responsibilities of the Supervisors, recall that those 3 regulators are the:

- Financial Markets Authority — the FMA supervises issuers of securities, trustee companies, futures dealers, collective investment schemes, derivatives and stockbrokers and financial advisors.
- Reserve Bank of New Zealand — the RBNZ regulates banks, life insurers, credit unions, and non-bank deposit taker firms.
- Department of Internal Affairs —the DIA supervises casinos, non-deposit taking lenders, money changers/remitters, cash security firms, debt collection and factoring, financial leasing, payroll, safe deposit, tax pooling and non-bank credit card firms. Since 2017, it has been changed with also supervising accountants, lawyers, real estate agents, the horse racing industry TAB, and dealers in high-value goods. The DIA is default Supervisor of other Reporting Entities not elsewhere supervised.

3.48. For some reporting entities, such as money remitters or lawyers, it has been something of a shock having to get accustomed to having a closer relationship with a highly proactive regulator. While for lawyers the NZ Law Society's Standards Committee system has been an effective regulatory arm for ethical issues, it is

set up to be largely reactive to complaints. Not so with the DIA, an agency that more regularly supervises and actively monitors what lawyers are up to in the area of AML compliance. That can extend to an on-site visit or a request for an external/independent audit to be conducted.

3.49. The DIA has published a guidance note (across all its regulatory fields, not specific to AML/CFT) which summarises its approach to compliance and enforcement.[22] It talks of the prioritisation models it will apply to its pool of regulated entities, and also available options and outcomes it may seek in its regulatory toolbox when needing to enforce or deal with non-compliance. The other Supervisors have similar high level enforcement priority statements available to those in sectors they regulate.

3.50. Formally, under s 131 of the AML/CFT Act, the functions of the AML/CFT Supervisors are to:

- monitor and assess the level of risk of ML/FT across all the Reporting Entities that it supervises;
- monitor those Reporting Entities for compliance with the AML/CFT Act and regulations, and for this purpose to develop and implement a supervisory programme;
- provide guidance to those Reporting Entities to assist those entities to comply with the AML/CFT Act and regulations;
- investigate those Reporting Entities and enforce compliance with the AML/CFT Act and Regulations;
- co-operate through the AML/CFT co-ordination committee (or other appropriate mechanism) with domestic and international counterparts to ensure the consistent, effective, and efficient implementation of the AML/CFT Act.

3.51. Turning to more enforcement oriented tasks, Supervisors have under s 132 of the Act all the powers necessary to carry out those main statutory functions, including to:

- conduct on-site inspections;
- provide guidance to the Reporting Entities it supervises by way of published guidelines, codes of practice, providing feedback on an entity's level of compliance with AML obligations, and undertaking any other activities necessary for assisting entities to understand their obligations and how best to achieve compliance with those obligations;
- on notice, require production of, or access to, all records, documents, or information relevant to its supervision and monitoring of Reporting Entities for compliance with the Act;
- co-operate and share information by communicating information (or making arrangements for that) obtained by the Supervisor in performing its functions and exercising powers under the Act;
- in accordance with the AML/CFT Act and any other legislation, initiate and act upon requests for assistance from any overseas counterparts; and
- approve the formation of, and addition of members to a Designated Business Group.

3.52. All the Supervisors, and especially the DIA, have become more active in issuing s 132 notices to demand the information needed in response to complaints, Police FIU feedback, their own monitoring activities, and investigations originating in other disparate sources or events. Note also s 133 of the AML/CFT Act regarding a Supervisor's on-site inspection powers - none of which, however, for a law firm reporting entity would override genuine legal privilege in client-attorney documents.

3.53. The Commissioner of Police (typically acting through the FIU) has separate powers and functions of its own under ss 142-144 of the AML/CFT Act, which are of a similar nature and can have an impact on the conduct of a reporting entity, as well as the actions of its Supervisor.

3.54. The AML/CFT regime also provides hefty powers of enforcement to the Supervisors. Enforcement action taken by Supervisors should be in proportion to the nature and severity of the compliance breaches, and

[22] *Minimising Harm - Maximising Benefit: The Department of Internal Affairs' Approach to Compliance and Enforcement* (2012), available at https://www.dia.govt.nz/Minimising-Harm-Maximising-Benefit.

they have publicly endorsed regulatory principles such as fairness, consistency and transparency. Of course, what that means in any given investigation or prosecution scenario can vary a great deal. Ideally, most actions taken by the Supervisors should be educational, providing guidance to and cooperating with Reporting Entities to ensure compliance. However, depending on the scale of non-compliance, more serious actions the Supervisors can take are set out in FMA, RBNZ and DIA joint *AML/CFT Supervisory Framework* (updated Nov 2019).[23]

3.55. The Supervisors subscribe to a "regulatory pyramid" concept, where most compliance enforcement should be low-end steps at the base of the pyramid, gently nudging Reporting Entities along the path to compliance. Salient features of the range of available steps in a sliding scale include:

- Education, co-operation and guidance — this has been the place that the DIA has started from, in dealing with both Phase 1 and Phase 2 transitions, before the enforcement approach gradually shifts up in gear from that low-key initial approach.
- Monitoring — this includes on-site inspections, desk-based reviews and research, and analysis of annual report information as filed by reporting entities.
- Investigations — the DIA may decide to carry out an investigation to identify any non-compliance of its own volition, or in response to complaint, information, police operations etc.
- Sanctions — a range of regulatory tools used to punish non-compliance, including issue of formal warnings (private, or publicly released to the media), seeking performance injunctions, restraining injunctions and enforceable undertakings.
- Civil liabilities — if there is failure by a reporting entity to meet AML/CFT obligations, Supervisors can apply to the High Court for an order directing compliance with or monetary payment in relation to an enforceable undertaking earlier obtained; or seek an interim injunction (mandatory/ performance or restraining) and sue for pecuniary penalties in court for civil liability acts.
- Criminal prosecutions —for more serious non-compliance matters, criminal prosecutions can be taken relating to suspicious transaction or wire/cash reporting failures, for obstructing or misleading supervisors, or failing to provide information to Supervisors or the Police FIU.
- Further, any of the civil liability acts defined in the AML/CFT Act (s 78) might also amount to criminal offences if they are conducted knowingly or recklessly by the reporting entity. Supervisors can in such cases choose whether to prosecute for criminal offences under the Act or by way of civil action.

[23] Available at AMLCFT-Supervisory-Framework-Nov 2019.pdf (rbnz.govt.nz).

4. CATEGORIES OF REPORTING ENTITIES, AND SUMMARY OF THEIR OBLIGATIONS

4.1. Whether a business is covered by the AML/CFT Act depends on whether it is deemed to be a "Reporting Entity" as defined in the Act. In substance, that turns on the extent to which it engages in specified regulated services or activities. The statutory definitions feeding into the question of who is a "Reporting Entity" are spread over several layers, requiring navigation of the s 5(1) interpretation provisions.

4.2. The priority areas in passing the 2009 Act were banking and financial service providers, a varied filed in itself. Extension to a wider set of professions was always anticipated, as "Phase 2" coverage. The government's intention when eventually passing the AML/CFT Amendment Act 2017 was that, with very few exemptions, most of New Zealand's 1,900 or so private practice law firms and sole practitioners would be covered as well as almost all real estate agents. As a result, it is assumed that almost all transactional or corporate law firms will be captured in at least one respect.

4.3. The path to ascertaining coverage for each Reporting Entity is essentially determined by three issues:

1) Whether it provides an AML-captured service in one of the defined ways/areas?
2) If so, whether it provides that service in the ordinary course of business?
3) Finally, whether any exemptions may apply?

4.4. Matters of interpretation and borderline issues can arise at any of those three steps above, so the answer to whether a particular type of business is in or out of scope is not always clear, and advice may have to be sought in answering the question "when and how does this Act apply to me?"

4.5. A key point to grasp is that capture as a Reporting Entity is "activity-based"- meaning coverage is determined by the type of activities engaged in, not by the label or structure of the entity itself. For example, in the case of lawyers coverage is not because the person is a lawyer, conveyancer, or law firm, or holds a Law Society-issued practising certificate. It is due to the particular legal services offered, and only to the extent those services are provided (s 6 of the Act). This means that for Phase 2 entities a close understanding of those activities, both their statutory wording and the intended ambit, is important.

Reporting Entity definitions

4.6. Starting at the broadest level, the coverage definitions applicable for all reporting entities are found throughout the interpretation section 5(1) of the AML/CFT Act – starting with broad categories of firms:

> "**reporting entity** -
> "(a) means-
> "(i) a casino:
> "(ii) a designated non-financial business or profession:
> "(iii) a financial institution:
> "(iv) a high-value dealer:
> "(v) TAB NZ ; and
> "(b) includes-
> "(i) a person or class of persons declared by regulations to be a reporting entity for the purposes of this Act; and
> "(ii) any other person that is required by any enactment to comply with this Act as if it were a reporting entity; but
> "(c) excludes a person or class of persons declared by regulations not to be a reporting entity for the purposes of this Act"

4.7. Each of those main umbrella categories, such as financial institution, high-value dealer, and designated non-financial business or profession (DNFBP), has its own separate definition in s 5(1), to elaborate further on what they each mean.

4.8. There is a sweeping list of covered activities carried out by financial institutions in para (a) of the definition of "financial institution" in s 5(1) of the AML/CFT Act. Those activities include:

> "(i) accepting deposits or other repayable funds from the public:
> "(ii) lending to or for a customer, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions (including forfeiting):
> "(iii) financial leasing (excluding financial leasing arrangements in relation to consumer products):
> "(iv) transferring money or value for, or on behalf of, a customer:
> "(v) issuing or managing the means of payment (for example, credit or debit cards, cheques, traveller's cheques, money orders, bankers' drafts, or electronic money):
> "(vi) undertaking financial guarantees and commitments:
> "(vii) trading for, or on behalf of, a customer in any of the following using the person's account or the customer's account:
> "(A) money market instruments (for example, cheques, bills, certificates of deposit, or derivatives):
> "(B) foreign exchange:
> "(C) exchange, interest rate, or index instruments:
> "(D) transferable securities:
> "(E) commodity futures trading:
> "(viii) participating in securities issues and the provision of financial services related to those issues:
> "(ix) managing individual or collective portfolios:
> "(x) safe keeping or administering of cash or liquid securities on behalf of other persons:
> "(xi) investing, administering, or managing funds or money on behalf of other persons:
> "(xii) issuing, or undertaking liability under, life insurance policies as an insurer:
> "(xiii) money or currency changing; …"

4.9. The AML/CFT regulations are amended from time to time, including the "Definitions" and "Exemptions" sets of regulations. This mechanism provides the government, in effect the Ministry of Justice, with flexible ability to clarify and expand upon the definitions by including or excluding particular roles, classes of activity, and service providers.

4.10. Turning to DNFBPs, s 5(1) of the Act has discrete and detailed definitions for sets of activities that may be engaged in by any of the professional groups: lawyers, accountants, real estate agents or conveyancers. Again, it is activities-based – such that an accounting firm or a law firm must figure out which of its teams or services fall into the definitions and therefore make it a reporting entity. Equally, if the firm chose to cease providing certain services or carrying out certain activities, it can limit or remove entirely the extent that those activities mean they are captured by the AML regime.

4.11. The sub-definitions in para (a) of the DNFBP definition control which activities are captured, and have some complexity so it is best to set them out in full:

> "**designated non-financial business or profession** means-
> "(a) a law firm, a conveyancing practitioner, an incorporated conveyancing firm, an accounting practice, a real estate agent, or a trust and company service provider, who, in the ordinary course of business, carries out 1 or more of the following activities:
> "(i) acting as a formation agent of legal persons or legal arrangements:
> "(ii) acting as, or arranging for a person to act as, a nominee director or nominee shareholder or trustee in relation to legal persons or legal arrangements:
> "(iii) providing a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal person or arrangement, unless the office or address is provided solely as an ancillary service

to the provision of other services (being services that do not constitute an activity listed in this subparagraph or subparagraphs (i), (ii), and (iv) to (vi)):

"(iv) managing client funds (other than sums paid as fees for professional services), accounts, securities, or other assets:

"(v) providing real estate agency work (within the meaning of section 4(1) of the Real Estate Agents Act 2008) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008):

"(vi) engaging in or giving instructions on behalf of a customer to another person for-

"(A) any conveyancing (within the meaning of section 6 of the Lawyers and Conveyancers Act 2006) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008), namely,—

"• the sale, the purchase, or any other disposal or acquisition of a freehold estate or interest in land:

"• the grant, sale, or purchase or any other disposal or acquisition of a leasehold estate or interest in land (other than a tenancy to which the Residential Tenancies Act 1986 applies):

"• the grant, sale, or purchase or any other disposal or acquisition of a licence that is registrable under the Land Transfer Act 1952:

"• the grant, sale, or purchase or any other disposal or acquisition of an occupation right agreement within the meaning of section 5 of the Retirement Villages Act 2003:

"(B) a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008); or

"(C) the transfer of a beneficial interest in land or other real property; or

"(D) a transaction on behalf of any person in relation to the buying, transferring, or selling of a business or legal person (for example, a company) and any other legal arrangement; or

"(E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement; …"

4.12. These definitions are a bit of a mouthful, even for lawyers, but it can be deduced that the main areas of attention from an AML risk and policy-making perspective (in simplified terms) are intended to be:

- real estate/conveyancing/property transactions;
- client funds and assets passing through a firm and its trust account;
- managing client funds, assets and affairs;
- setting up, directing and running companies or trusts (registered office/secretariat services etc); and
- merger/acquisition or sale and purchase of companies, trust assets and the like.

4.13. Preliminary points to reinforce include that the activities of DNFBPs listed in s 5(1) of the AML/CFT Act apply across DNFBP types regardless of which profession is caught. This allows for the possibility of multi-disciplinary practices, or overlap in services. So, it could be an accountant or a lawyer setting up companies and trusts; and it could be a lawyer, conveyancer or real estate agent selling a property. The close relationship in a property transaction between real estate agent, mortgage funder, and conveyancing lawyer was in all likelihood intended to ensure one or more angles would always catch such transactions. There is often duplication, as an unfortunate result. But in substance the overlaps emphasise that what you do as a regulated activity is what matters.

4.14. There is the prospect of this DNFBP definition being adjusted to include parties declared by regulations to be in or out of scope. Section 154 of the AML/CFT Act allows for the Governor-General by Order in Council to make regulations that declare a person or class of persons to be or not be a reporting entity for the purposes of the Act. An example of this during Phase 1 was the specific exclusion of lawyers to ensure they

were not caught by reason only of carrying out a relevant financial service in the course of legal professional work. Once lawyers were brought in by Phase 2, that was no longer necessary.

4.15. Some parts of the defined activities are very precise, cross-referencing to other statutory definitions such as in the Real Estate Agents Act 2008. Conversely, other parts of the language are open to interpretation and perhaps deliberately kept broad and general – for example, the broad scope of "giving instructions on behalf of a customer to another person … in relation to [a transaction for] any other legal arrangement" is a matter on which opinion can vary. Many of these areas will lead to interpretative uncertainty to be worked out over time. Guidance notes from each Supervisor help reduce uncertainty by setting out the regulators' opinion, but ultimately only a Court (or alternatively an exemption) can confirm the ruling on coverage.

DIA has the coverage of the widest range of sub-sectors

4.16. This table below summarises the current sub-sectors which the DIA, as largest Supervisor, assesses and regulates.[24] The left side column labels the sub-sector in practical, functional terms. Virtual asset service providers, including cryptocurrency providers, brokers, exchanges and intermediaries, have only recently been treated as captured. Rather than a formal amendment or new Regulation including that sector, the DIA simply announced on its website that it was now interpreting the limb of the financial institution definition that states: "*issuing or managing the means of payment (for example, credit or debit cards, cheques, traveller's cheques, money orders, bankers' drafts, or electronic money)*" to cover the crypto-sector.

4.17. The right hand column and colour coding represents the current assessed inherent money laundering and terrorist financing risks of each sector, as the DIA perceives it in 2019:

Sector - Financial Institutions	**Inherent risk of Money Laundering / Terrorist Financing**
Money remittance	High
Virtual asset service providers	High
Currency exchange	Medium-high
Payment provider	Medium-high
Non-bank non-deposit taking lenders	Medium
Non-bank credit cards	Medium
Stored value cards	Medium
Cash transport	Medium
Tax pooling	Low
Debt collection	Low
Factoring	Low
Financial Leasing	Low
Payroll remittance	Low
Safe deposit boxes	Low
Sector – Designated Non-Financial Businesses or Professions (DNFBPs) and casinos	
Trust and company service providers	High
Lawyers	Medium-high
Accountants	Medium-high
Real estate agents	Medium-high
High-value dealers	Medium-high

[24] Adapted from the Department of Internal Affairs *Financial Institutions Sector Risk Assessment*, December 2019, at p6.

Racing Industry Transition Agency (TAB)	Medium-high
Casinos	Medium-high
Conveyancers	Medium

4.18. Each of the Supervisors is required to put out periodic Sector Risk Assessments of this type, risk-rating the perceived level of ML vulnerability that businesses in each sub-sector may face. Reporting Entities are expected to then take guidance and cues from the specific materials put out by their Supervisor considered pertinent to risks in their areas of business.

Occasional activities – is it in a firm's "ordinary course of business"?

4.19. A further important qualification on coverage is that a person who carries on one or more of those defined activities is captured if they do that "in the ordinary course of business" – see the s 5 definition. Accordingly, whether they will have to comply with the AML/CFT Act's extensive list of obligations may depend entirely on this rather vague phrase.

4.20. The AML/CFT Act does not define that meaning and, to date, no Court analysis or precedent helps take this further. In that vacuum, the Supervisors issued a guideline to clarify how they intend to apply the phrase "ordinary course of business". That document sets out a number of quite logical contextual factors, which, when considered together, may indicate whether or not an activity is in the usual course of business for each potentially captured firm.

4.21. The purpose lying behind this appears to be that dabbling infrequently in a regulated activity, or as a one-off, should not necessarily attract the full compliance burden of the AML regime. Even so, this guidance document affords a lot of room to interpret and weigh factors in different ways. There is no bright-line test to apply to determine "ordinary course of business".

4.22. These factors involve whether the legal service/activity:

- is normal or otherwise unremarkable for the firm (including as indicated by the firm's internal processes, staff training and systems, and marketing materials);
- is frequent or is regular (even if infrequent, it could be a predictable, annual event);
- involves significant amounts of money and transaction value;
- is a source of revenue for the firm (even if small);
- involves significant allocation of the firm's resources; or
- involves a service or product that is offered to customers or third parties.

4.23. The Supervisors have emphasised that no one factor overrides the assessment. They must all be taken together, and some factors may need to be off-set or have to be weighed against each other.

Exemptions

4.24. The AML/CFT Act itself is deliberately broad in what it covers. A wide sweep of routine financial, transactional and legal activities are treated as covered services. However, to mitigate the broad sweep of what is covered, some aspects have then been carved out by specific detailed regulatory exemptions. This has been done mostly via delegated legislation but often in a piecemeal way as and when an over-reach issue is noted or a sector lobbies for it. These are typically for a whole class or category of matters, usually but not always with formal consultation before promulgation in the published Statutory Regulation series.

4.25. Separate to regulated or class exemptions of general applicability, there is a system for entities on the borderline to apply for specific exemption, described as the "Ministry of Justice bespoke exemptions" process. This can be very important to taming the threat of over-reach and inadvertent capture under the AML regime. An application process and format exists to by prepared and lodged with the Ministry,

including a variety of particular factors and tests that need to be addressed, and against which the Ministry evaluates applications for exemption.

4.26. Obviously a key factor is actually the correct/best interpretation of the definitions and how they apply to any law firm scenario, and whether the likely level of money laundering risk can be persuasively presented as low, but other factors affecting the public interest and overall integrity of the regime are evaluated.

4.27. In form, the Minister of Justice eventually grants an exemption, via a regulatory process published in the Official Gazette of New Zealand. But in practice, Ministry officials run the application process, with involvement of Supervisors, and their recommendation carries sway in the outcome of the process.

4.28. As at the end of March 2021 there have been a total of over 140 bespoke exemptions granted at different times as listed on the Ministry website. Additionally, there remains quite a pipeline of pending applications not yet determined, and hence not yet on that list of those that have been granted. Some are for full exemption from the Act, some just for partial relief from certain specified obligations that may be causing particular problems for the entity in question.

If covered as a Reporting Entity, what are the main legal obligations?

4.29. Some key obligations were already addressed in part 3 of this report. The other range of statutory requirements upon reporting entities are mainly contained in ss 56-58 of the AML/CFT Act, although scattered elsewhere in the Act and Regulations too.

4.30. Leaving aside the specific basic issues that were addressed earlier – the role of the AMLCO, senior management governance, the written risk assessment and review/audit/annual report obligations - we might summarise and simplify the remaining major compliance obligations as a reporting entity must:

a. Establish, implement, and maintain an AML/CFT compliance programme, based upon the risk assessment done earlier. The programme must include a variety of specific minimum aspects to it, as detailed in s 57 of the Act.

b. Put in place internal procedures to ensure that standard Customer or Client Due Diligence ("CDD") measures are carried out, when commencing a new business relationship or carrying out an occasional transaction for all new clients onboarded, and after a time any existing clients that have been with the entity prior to the commencement of its AML/CFT obligations as a captured reporting entity.

c. Develop mechanisms to determine if more stringent, enhanced CDD measures are required - for example, if dealing with trusts, wire transfers, high risk countries, or Politically Exposed Persons ("PEPs") - who are certain types of prominent foreign public figures. Much of the media fuss after the Panama Papers focused on these types of politician, billionaire or kleptocrat clients.

d. Carry out training, and recruitment vetting, for staff involved in AML procedures.

e. Apply ongoing due diligence and transaction monitoring processes, to all clients (new or existing) and especially to any identified as high risk in your risk assessment.

f. Make Suspicious Activity Reports ("SAR") and co-operate with supervisors and the Police agencies – and without disclosing anything to the client about the SAR - and make regular Prescribed Transaction Reports ("PTR") if required. PTRs are made regardless of any suspicion, for all cash transactions or international wire transfer transactions made through the entity if over specified dollar thresholds.

g. Ensure safe retention of various types of records (client, compliance, transactions) for a minimum number of specified years.

h. Make an annual report to the Supervisor on the firm's compliance with its AML/CFT programme, and also have a biennial independent audit carried out of its compliance performance. These intrusive external dives into the law firm's compliance environment are designed to detect poor systems against money laundering, and promote self-reporting of any breaches.

4.31. As noted, there are a lot more specific or contingent obligations contained in the Act and Regulations too, depending in part on what the reporting entity may do and how it organises its affairs.

Customer Due Diligence – verifying identity, ownership, purpose of customer relationship

4.32. A key feature of AML regimes around the world is to force reporting entities to develop more detailed processes by which to understand their customers more deeply, by several types of Customer Due Diligence ("CDD") - known overseas more commonly as KYC ('know your customer') checking processes.

4.33. While there is room to apply a risk-based approach, allowing flexibility in some areas according to the circumstances, there are also minimum requirements set out in the New Zealand AML/CFT Act. Sections 10 to 17 contain the main requirements for standard CDD, and also additional relaxations in certain circumstances for simplified CDD (ss 18 to 21), and more stringent requirements for enhanced CDD where the situations might be deemed a higher risk (ss 22 to 30).

4.34. Generally, the CDD required when the law was implemented was not retrospective: it did not require all existing customers to be reinvestigated so as to become verified upon the law coming into force, only new customers henceforth. There were some exceptions - if and when the nature of the relationship changes, or suspicion is raised, or an entity realises it holds inadequate or anonymous account information. But by and large the law allowed the rump of pre-existing customers to be addressed gradually over time using another form of due diligence termed Ongoing CDD (s 31).

4.35. CDD will typically apply to onboarding new customers or accounts where a business relationship is established having an element of duration, or occasional transactions are conducted as a one-off outside of a business relationship over a threshold (NZ $1000).

4.36. Under s 11 CDD must be performed on each of three 3 types of person: the actual customer/client; beneficial owners of a customer/client; and any person acting on behalf of a customer/client. Information must also be obtained on the nature and purpose of the customer's intended relationship with the entity.

4.37. "Beneficial owner" can be a messy concept to understand and apply. As defined for AML/CFT purposes it means an individual who has effective control of a customer, or a person on whose behalf a transaction is conducted; or who owns more than a prescribed threshold level of anything over 25 % of the company/partnership or entity. If the immediate owners are corporate entities, the reporting entity must continue to follow chains of ownership so that it knows and understands who are the individual persons ultimately owning the customer.

4.38. Section 15 sets out the minimum information required for standard CDD: the person's full name, date of birth, if not the customer, that person's relationship to the customer, address or registered office and the person's company identifier or registration number, as well as any information prescribed by the Regulations. The entity must first collect and then take reasonable steps verify that information using details and documents that are reliable and depending on the level of risk in certain situations (or as prescribed in Regulations). Guidance has been issued on CDD variations for individuals, company, trust, partnership, co-operative, charity and other types of entity.

4.39. An Identity Verification Code of Practice was issued by the Supervisors in 2013, amended and updated since. It contains detailed options of the type of documentary evidence or electronic verification methods that may be considered acceptable, including biometric features. It is for use when verifying the identity of

low to medium risk individuals, not companies or high risk customers. The Code is not compulsory but, if followed, acts as a safe harbour, providing a way of showing compliance with the AML/CFT obligations.

Enhanced CDD and beneficial ownership – understanding source of funds or wealth

4.40. Reporting entities must still consider more closely, and take additional CDD measures in relation to any high risk customers or situations they encounter. For the most part, those extra measures involve steps to ascertain (and verify) the customer's source of wealth (i.e. assets) and/or source of funds for a transaction.

4.41. Section 22 and 22A of the AML/CFT Act set out when a firm will need to conduct Enhanced CDD – a description of those high risk areas. As well as doing Standard CDD identity checks there must be some additional checking, but the extent of that additional level of enquiry and validation of answers is not prescribed, rather it is left to be decided by the entity applying its risk assessment principles and ratings.

4.42. The triggers in the AML/CFT Act (which can be potentially supplemented by Regulations) for Enhanced CDD are varied, and not all will apply to all firms. But some key triggers are scenarios (adapted from FATF recommendations) where:

a. a customer (or a beneficial owner) is a trust, or other vehicle for holding personal assets, s 22(1)(a)-(b).

b. a customer is a non-resident customer from a high risk jurisdiction – i.e. one with insufficient AML-CFT systems or measures in place, s 22(1)(a)-(b).

c. a customer is a company with nominee shareholders or shares in bearer form, s 22(1)(a) and (b).

d. a customer seeks to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose, s 22(1)(c).

e. a customer is a Politically Exposed Person ("PEP"), under s 22(2).

4.43. The main practical point of the additional checking that Enhanced CDD requires is to understand the source of funds, assets or wealth that the customer has behind them or is seeking to use to conduct the transaction/activity in question. Entities have in practice struggled without a clear signalling device or criteria in the Act as to what constitutes sufficient proof of source of funds (and hence there is wide variation of practice, even with detailed Supervisor guidelines).[25] The difficulties are reinforced under s 37 of the AML/CFT Act with obligations to terminate a customer relationship, or not carry out a transaction, if the requisite form of Enhanced CDD cannot be conducted, or is started but cannot be completed.

4.44. Beneficial ownership is a challenging area of compliance in New Zealand, given the relatively diverse and high proportion of trust structures used in commercial and property enterprises. A balance has been struck in the AML/CFT Act and Regulations that will require entities to verify beneficial ownership by obtaining the name and date of birth of each beneficiary of a trust or, for charitable or discretionary trusts with more than 10 beneficiaries, a description of the class and types of beneficiary and trust objectives.

4.45. Many trust structures or vehicles for holding assets exist for benign and legitimate purposes. But the extent to which permeate our commercial and real estate asset base can lead to complications and customer resistance for firms trying to carry out the necessary levels of Enhanced CDD. A Guidance Note indicating the Supervisors' approach to beneficial ownership was issued in 2012, [26] but of necessity it is quite generalised. Without any moves yet to create a beneficial ownership register, as some countries are now implementing, getting access to publicly verifiable data in these scenarios can be difficult. Even when the local ownership can be checked, it may often have overseas strands, given the high level of foreign investment in New Zealand, and few means of verifying overseas beneficial ownership information.

[25] FMA, RBNZ, DIA – Joint Supervisors *AML/CFT Enhanced Due Diligence Guideline*, updated September 2020, available at: https://www.fma.govt.nz/compliance/guidance-library/amlcft-enhanced-customer-due-diligence-guideline/

[26] FMA, RBNZ, DIA – joint Supervisors "AML/CFT – Beneficial Ownership Guideline", December 2012, pg 3.

4.46. That Guidance on this topic confirms the beneficial owner individual search obligations in these terms:

> "12. Your obligation is to determine the individual(s) who are the beneficial owner(s). A beneficial owner is an individual (a natural person). Therefore the beneficial owner can only be an individual, not a company or organisation. There may be more than one beneficial owner associated with your customer. Your task is to identify and verify the identity of all the beneficial owners of your customer.
> …
> 16. There may be individuals who have effective control … over the customer, but do not have an ownership interest and are not a person on whose behalf a transaction is conducted; they will be beneficial owners. Effective control, ownership and persons on whose behalf a transaction is conducted are not mutually exclusive."

4.47. Assuming the requisite levels of CDD are navigated, a reporting entity must then under s 31 of the Act conduct Ongoing CDD and undertake Account Monitoring, to ensure that the business relationship with the client and transactions carried out turn out to be consistent with their prior knowledge about the client, its business and risk profile. An important additional purpose to the monitoring is to identify grounds for reporting any suspicious activity or a suspicious transaction. I address the SAR requirements more in part 5 of this report below.

4.48. Ongoing CDD is more of a refresh and updating process, serving to check that information previously obtained about clients remains correct, up to date, and valid.

4.49. Reporting entities are required to keep many types of transaction records, CDD identity and verification records, records relevant to its risk assessment, compliance programme and audits, and also records relevant to the nature, purpose and establishment of business relationships established.[27]

Practical difficulties with the more complex types of due diligence

4.50. As might be expected with the implementation of any complex new regulatory regime, reporting entities and their customers have had plenty of teething troubles to grapple with during the early years of the AML/CFT Act regime. Many of the same concerns, along with a lack of understanding of the nuances of Supervisor expectations, played out again for Phase 2 entities from 2018 onwards. In particular, there has been considerable over aspects of Enhanced CDD rules, especially as they apply to trusts or other high-risk and complex ownership situations.

4.51. Standard CDD checking, by means of a passport, driver's licence, or other forms of verification permitted under the Code of Practice, is by and large able to be accommodated well. But duplication abounds, and customers' transactions are often slowed and more costly when non-standard verification scenarios arise.

4.52. Account or activity monitoring also proves easy to say in law, but difficult to do in practice. Banks and large institutions spend greatly on automated software and systems but still frequently get the details wrong or miss important red flags. And even reputable law firms' trust accounts have raised concerns among mainstream banks about the lack of visibility a bank has into the actual transactions and co-mingling of funds that inevitably takes place through it.

4.53. The law in a number of areas of deep detail is unnecessarily complex, in my view. This ends up driving confusion and variable practice across sectors, and sometimes even across the 3 Supervisors and the Police FIU. The outcome is higher than necessary compliance costs for many small-medium sized businesses.

4.54. How the regulators grapple with this problem and whether they strive to simplify the legal obligations will be a critical issue in an upcoming statutory review process scheduled to take place in 2021. The complexity and inconsistencies of the multi-Supervisor model, and regulators' inherent tendency to incrementally layer in more levels of detail, more acronyms, and highly-nuanced guidance notes, have not assisted entities to readily interpret and apply the fluid risk-based approach. That too ends up creating problems of cost and accessibility to the law for smaller enterprises, and their customers.

[27] Details are in subpart 3 of part 2 of the AML/CFT Act.

5. APPLICATION OF THE AML/CFT REGIME TO THE LEGAL PROFESSION, AND THE RELATIONSHIP WITH LAWYER-CLIENT PRIVILEGE

5.1. As explained in part 3 of this report, lawyers were the first professional sector of the Designated Non-Financial Business and Profession ("DNFBP") categories to be advanced into the AML regime as part of Phase 2 reforms. The AML/CFT Act has been applied in full to law firms of all sizes who provide any of the captured services from 1 July 2018. Subsequent staged implementation times then transitioned into the regime the other non-financial sectors: accountants, real estate agents, licenced conveyancers, the TAB totalisator gaming body, and selected dealers in high-value assets.

5.2. In part 4 above, I explained how the *Shewan Report* and examples disclosed in the Panama Papers case studies highlighted risks for legal service providers, especially around property transactions, trusts and opaque corporate structures. A particular concern was that New Zealand's renowned ease of doing business, and safe reputation, including favourable tax settings for foreign or offshore trusts, was attracting criminal groups and agents who may seek to place and layer money for cleansing through this country.

5.3. Lawyers may have been targeted by sophisticated laundering operations precisely because they were exempt from 2013 to 2018, when ordinary businesses or lay persons who offered the same trust and company secretarial services were caught by the Phase 1 changes since 2013. Criminals and their agents would move around to avoid the greater information demands which financial businesses were compelled to make from those customers. This led to a displacement effect, potentially just shuffling the laundering issues from one set of providers to another, in order to avoid the new regulatory net.

5.4. Those core activities - establishing trusts and companies, secretariat, transactional and trust account administrative services offered, alongside substantive law work for clients in real estate, business sales and finance, trust, asset planning or tax structuring fields - were intended to be captured by a number of the defined limbs of activity. In other words, a lot of bread-and-butter legal work for firms of solicitors was seen as central to the money laundering risk.

5.5. Recall that coverage is determined by whether any of a defined set of activities is performed. Other peripheral, less risky legal fields might be non-captured services, so some things done by a lawyer remain outside the AML obligations - e.g. litigation work is generally out of scope. This adds complexity, especially for full-service law firms when only some services are covered and therefore attract AML obligations of KYC/CDD, ongoing monitoring, SAR and PTR reporting etc.

5.6. However, it also provides useful dividing lines between transactional legal services and court or dispute resolution work that could otherwise cause more intense ethical dilemmas – e.g. criminal defence representation of an accused, if that does not involve holding funds in trust account for other purposes, should be out of scope.

Misuse of legal services for criminal ends may unwind client fidelity and privilege duties

5.7. A particular difficulty that lawyers have, which no other sectors of captured reporting entities face, is the strong ethical duties owed to the client, including as to keeping confidences and upholding legal privilege in communications. The AML regime took care to recognise that difficulty when coverage expanded in 2017.

5.8. That perceived sanctity of legal professional privilege, and ethical duties such as utmost fidelity and loyalty to the client, has never been absolute. The common law has always recognised exceptions to privileged

communications, and some of those exceptions find a clear place in the New Zealand rules of professional conduct for lawyers, where an admitted barrister or solicitor's overriding duty is to the Court.[28]

5.9. Under our Rules of Conduct & Client Care ("RCCC"), a series of provisions exhort lawyers to:

- use legal processes only for proper purposes - RCCC, r 2.3;
- not to assist any person in activity the lawyer knows to be fraudulent or criminal, and not to knowingly assist in the concealment of fraud or crime - RCCC, r 2.3;
- consider whether they should disclose confidential information (using permissive language, *may* not "must") relating to the business or affairs of a client where it: relates to the anticipated commission of a crime of fraud (RCCC, r 8.4(b)); or is reasonably believed to relate to past use of legal services for crime or fraud - and where it is necessary to disclose to avoid the types of loss/harm to others that are mentioned in the Rules (RCCC, r 8.4(d)).

5.10. It can be seen that balancing other competing legal, criminal law or interests of justice factors is always part of the process. The Panama and Paradise Papers and related scandals, including those involving misuse of New Zealand trusts and shell companies, suggests some lawyers may have elevated notions of duties to the client above the balancing act that is really required.

5.11. Well before those international scandals came to light, the FATF had clearly set out concerns over abuse of lawyers, and legal privilege specifically, in a 2013 report on *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professional*: [29]

> "… criminals seek out the involvement of legal professionals in their ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism. "The report identifies a number of ML/TF methods that commonly employ or, in some countries, require the services of a legal professional. Inherently these activities pose ML/TF risk and when clients seek to misuse the legal professional's services in these areas, even law abiding legal professionals may be vulnerable." (page 4)

- and further, regarding privilege and professional secrecy:

> "… the perception sometimes held by criminals, and at times supported by claims from legal professionals themselves, that legal professional privilege or professional secrecy would lawfully enable a legal professional to continue to act for a client who was engaging in criminal activity and/or prevent law enforcement from accessing information to enable the client to be prosecuted. However, it is apparent that there is significant diversity between countries in the scope of legal professional privilege or professional secrecy. Practically, this diversity and differing interpretations by legal professionals and law enforcement has at times provided a disincentive for law enforcement to take action against legal professionals suspected of being complicit in or wilfully blind to ML/TF activity." (page 6)

5.12. Most jurisdictions, including New Zealand and Australia adopt versions of the principle to the effect that legal professionals must not engage in, or assist their client with, conduct that is intended to mislead or adversely affect the interests of justice or enable fraud or criminal activity. That is considered antithetical to the foundation stone of legal professional practice in upholding the interests of justice. In short, fraud, corruption or criminality can pierce a major hole in the protective blanket of legal privilege. That has been the case long before AML regulation came along.

Privilege and confidentiality still exists, uneasily, alongside SAR obligations

5.13. Although able to be pierced by exceptions, the legal profession is still built upon fundamental duties (some would say, human rights) that include the right of a client to receive private legal advice which can be with-held from all, even a Judge. That includes corresponding duties of a lawyer to maintain strict confidentiality in that information, alongside fidelity to the client and his/her right to legal professional privilege.

---

[28] Lawyers: Conduct and Client Care Rules 2008 (RCCC), a set of Regulations made under delegated authority of the Lawyers and Conveyancers Act 2006, comprising the ethical code for regulation of all lawyers admitted in New Zealand.

[29] *FATF, Money Laundering and Terrorist Financing Vulnerabilities of Legal Professional*, June 2013, available at https://www.fatf-gafi.org/documents/documents/mltf-vulnerabilities-legal-professionals.html.

5.14. Those duties are much more than superficial; they are obligations set at a fiduciary level, and regarded as substantive rights not to be derogated from in the absence of clear legislative intent. Such specific legislative intent, albeit in cautious fashion, can be seen at work in the AML/CFT Act reporting obligations.

5.15. The obligation to make a SAR is found in s 40 of the AML/CFT Act, fleshed out by the definitions in s 39A. In simplified terms, if a lawyer (or any reporting entity) has "reasonable grounds to suspect" that activity or a transaction, or even a proposed transaction/activity/mere inquiry about services, is or may be related to crime, money laundering, criminal proceeds, or terrorism, it must report securely and speedily to Police.

> **40 Reporting entities to report suspicious activities**
>
> "(1) Subsections (3) and (4) apply to reporting entities other than high-value dealers.
>
> (2) [*omitted*].
>
> (3) If this subsection applies, the reporting entity must, as soon as practicable but no later than 3 working days after forming its suspicion, report the activity, or suspicious activity, to the Commissioner in accordance with section 41.
>
> (4) Nothing in subsection (3) requires any person to disclose any information that the person believes on reasonable grounds is a privileged communication.
>
> **39A Interpretation**
>
> **"suspicious activity** means an activity undertaken in circumstances—
>
> (a) in which—
>
> (i) a person conducts or seeks to conduct a transaction through a reporting entity; or
>
> (ii) a reporting entity provides or proposes to provide a service to a person; or
>
> (iii) a person requests a reporting entity to provide a service or makes an inquiry to the reporting entity in relation to a service; and
>
> (b) where the reporting entity has reasonable grounds to suspect that the transaction or proposed transaction, the service or proposed service, or the inquiry, as the case may be, is or may be relevant to …"

5.16. Most importantly, s 40(4) is unequivocal in preserving a right not to disclose privileged communications.

5.17. This obligation to make SARs and effectively "dob in" a client, has been an area of real anxiety for lawyers as they came under the AML/CFT regime for the first time. Understandably so, for these are among the most difficult judgement calls to be made across the whole field of AML obligations. Having to decide to report on a client goes against the grain of core training for many lawyers. These issues are going to be complex and multi-factored, sometimes deserving of an external sounding board or independent advice. But although complex, the issues are not irreconcilable.

5.18. It is crucial to note that privilege still exists in the AML/CFT regime, and is protected, where the information is truly privileged. There is no requirement to submit SARs when privilege or secrecy genuinely applies.[30]

5.19. Following the separate Evidence Act 2006, s 42 of the AML/CFT Act defines what amounts to a privileged communication:

> (1) A communication is a **privileged communication** if -
> (a) it is a confidential communication (oral or written) (including any information or opinion)—
> (i) that passes between –
> (A) a lawyer and another lawyer in their professional capacity; or
> (B) a lawyer in his or her professional capacity and his or her client; or
> (C) any person described in subparagraph (A) or (B) and the agent of the other person described in that subparagraph (or between the agents of both the persons described) either directly or indirectly; and

[30] *Suspicious Activity Reporting Guideline 2018*, NZ Police FIU, available at: https://www.police.govt.nz/sites/default/files/publications/suspicious-activity-reporting-guideline.pdf.

(ii) that is made or brought into existence for the purpose of obtaining or giving legal advice or assistance; or

(b) it is a communication (including any information or opinion) that-

(i) is subject to the general law governing legal professional privilege; or

(iii) is specified in section 53, 54, 55, 56, or 57 of the Evidence Act 2006."

5.20. So far, relatively uncontroversial. However the following part, s 42(2) in the Act, is possibly more important, with express spotlight on what is *not* privileged. None of this is especially revolutionary, but there has been a tendency by clients (and some lawyers) to assume that every communication with a lawyer attracts privilege - regardless of whether it is a substantive or mechanical piece of correspondence, and regardless of its purpose. That is not, and at common law has never been, the true position:

"(2) However, a communication is not a privileged communication -

(a) if there is a prima facie case that the communication or information is made or received, or compiled or prepared -

(ii) for a dishonest purpose; or

(iii) to enable or aid the commission of an offence; or

"(b) if, where the information wholly or partly consists of, or relates to, the receipts, payments, income, expenditure, or financial transactions of any specified person, it is contained in (or comprises the whole or a part of) any book, account, statement, or other record prepared or kept by the lawyer in connection with a trust account of the lawyer within the meaning of section 6 of the Lawyers and Conveyancers Act 2006.

(3) For the purposes of this section, references to a **lawyer** include a firm in which the lawyer is a partner or is held out to be a partner."

5.21. The policy rationale is reasonably clear: lawyers are primarily actors in the administration of justice and officers of the Court; privilege is about confidentiality and professional assistance with legitimate matters of justice; so helping in a crime or for a dishonest purpose is not true legal assistance of the kind the law should respect. And the privilege exists for genuine advice to the client, not administrative paperwork.

5.22. The *DIA v Ping An* case[31] (discussed in part 8 of this report) declared that an entity's decision to make a SAR engages an objective test. In other words, the "reasonable grounds to suspect" level of suspicion in s 39A is a threshold that is not left entirely up to the lawyer's subjective view – the courts and regulators may well come back and scrutinise the reasonableness of the suspicion formed (or ignored). This has been confirmed in a more recent criminal prosecution case also.[32] Together, these early prosecutions (admittedly, one undefended, and involving non-lawyer entities) indicate that the stakes are high.

5.23. Highlighting these new realities of life, the New Zealand legal profession has to face the harsh side of financial crime laws publicly affecting a few of its members, including the recent blemishes of:

- a former lawyer convicted and in jail for corruption offences in mortgage fraud cases in 2018;[33] and
- another lawyer who carried out work for the Comancheros motorcycle gang convicted in 2019 of money laundering offences, and sentenced alongside a gang member for money washing through his trust account to purchase assets.[34] See part 8 of this report for more discussion of this case.

5.24. In my practice, when advising law firms and busy commercial practitioners, facing up to the need for an imminent SAR is stressful and often they require specialist guidance, especially mindful of the strict 3-working days deadline for filing reports with the Police. Banks, by contrast, simply report automatically, without hesitation. But with clear thinking, senior practitioners in the firm looking at the issues, and willingness to consult with a trusted independent advisor, in my experience most of the issues can be worked through – delicately, but according to principled analysis of the proper law of privilege.

---

[31] *Department of Internal Affairs v Ping An Finance (Group) NZ Company Ltd, and Xiaoln Xiao* [2017] NZHC 2363.

[32] *R v QF, FC and JFL* [2019] NZHC 3058.

[33] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12100038.

[34] https://www.stuff.co.nz/national/crime/117656160/lawyer-admits-money-laundering-allegedly-linked-to-comancheros-motorcycle-club

6. A CRIMINAL PROCEEDS RECOVERY REGIME DOVETAILS WITH THE AML REGIME

6.1. The Criminal Proceeds (Recovery) Act 2009 ("CPR Act") sets out a detailed legislative scheme relating to asset freezing and forfeiture orders for property that might represent the proceeds of crime. Unlike older forfeiture laws in the shape of the Proceeds of Crime Act 1991, a criminal conviction is not required for the imposition of a restraining order or a forfeiture order.

6.2. All that is required for orders against criminal proceeds is proof of "significant criminal activity", on the civil standard of the balance of probabilities.

6.3. Significant criminal activity means activity that would amount to either an offence punishable by a term of imprisonment of 5 years or more, or from which property or proceeds of NZ$30,000 or more have been directly or indirectly obtained.

6.4. Until 2015, the AML/CFT Act also contained a definition that acted as a trigger for reporting of suspicious activity where the underlying predicate offence was thought to be a serious one, that engaged potential imprisonment of 5 years or more. To increase the catchment of intelligence material for reporting to the Police, that threshold of "serious offence" was removed, such that any level of offending can found a basis to make a suspicious activity report. But the threshold of 5 years' prison sentence remains in the CPR Act.

6.5. The purpose statement of the CPR Act (contained in s 3) is instructive as to why it was developed and gives clues as to why it is such a powerful weapon against organised crime:

> (1) The primary purpose of this Act is to establish a regime for the forfeiture of property—
> (a) that has been derived directly or indirectly from significant criminal activity; or
> (b) that represents the value of a person's unlawfully derived income.
>
> (2) The criminal proceeds and instruments forfeiture regime established under this Act proposes to—
> (a) eliminate the chance for persons to profit from undertaking or being associated with significant criminal activity; and
> (b) deter significant criminal activity; and
> (c) reduce the ability of criminals and persons associated with crime or significant criminal activity to continue or expand criminal enterprise; and
> (d) deal with matters associated with foreign restraining orders and foreign forfeiture orders that arise in New Zealand.

6.6. Using that as a guide to interpretation, the Supreme Court has described the purpose of "eliminating the chance to profit" as being liberally interpreted in that light - the "aspirational language" giving a "clear and emphatic signal as to the legislative purpose."[35]

6.7. It shares the objective of deterring criminal activity with the AML/CFT Act, which speaks of detecting and deterring money laundering behaviour. At a policy level, one system generates intelligence from the financial community about financial crime (and hence underlying criminal activity), and the other system uses that intelligence to direct operations that will strip out the profits/benefits of such criminal activity.

Orders available to the Commissioner of Police

6.8. Several types of orders are available under the CPR Act upon application by the Commissioner of Police, including asset forfeiture orders, profit forfeiture orders and instrument forfeiture orders. Prior to forfeiture, the CPR Act provides for restraining orders to freeze assets and property, for what can be potentially a long period until court outcomes are finally determined. They are used extensively by the Police, usually on a without notice (*ex parte*) application at the outset of an intended case.

---

[35] *Marwood v Commissioner of Police* [2016] NZSC 139, [2017] 1 NZLR 260 at [12].

6.9. The police can then apply for a civil forfeiture order in respect of certain property, including orders relating to both assets and profits. If the High Court (as main first instance hearing forum) is satisfied on the balance of probabilities that the items of property in question are "tainted" property, it must make an order. "Tainted property" is defined to include property that has wholly or in part been acquired as a result of significant criminal activity or directly or indirectly derived from significant criminal activity.

6.10. The effect of an assets forfeiture order is to formally vest the property in the Crown.

6.11. If it is shown that a respondent has benefited from significant criminal activity, and has an interest in property, then the Court must make a profit forfeiture order. These are not as frequently sought as an asset forfeiture order, but are potentially more flexible. Under s 55, the Court must make such an order if satisfied on the balance of probabilities that a person has unlawfully benefited from significant criminal activity during the 7 years immediately prior to the filing of the application and has interests in property.

6.12. Section 54 provides that the maximum recoverable amount under a profit forfeiture order is the value of the unlawful benefit less the value of any property forfeited to the Crown as a result of an assets forfeiture order made in relation to the same criminal activity. The purpose of this is to prevent double recovery, such that if an asset forfeiture order has been or is concurrently made, the terms of any profit forfeiture order must be adjusted to reflect that impost.

6.13. The CPR Act does not prescribe how the amount of any unlawful benefit is to be assessed by the Court. Instead, it operates by a statutory presumption in favour of Police if they state a reasonable value of claim/offending in their application (see s 53 for the presumption). Under s 53, the Commissioner of Police carries an initial burden of proving on the balance of probabilities that the responding party unlawfully benefitted from significant criminal activity, during a relevant period of criminal offending. It then falls to the respondent to rebut the statutory presumption (again, on balance of probabilities) that they have benefitted to the value claimed by the Police.[36]

6.14. If made, a profit forfeiture order is enforceable as an order made as a result of civil proceedings instituted by the Crown against the person to recover a debt due to it. Relief can be granted following application by affected third parties (other than the respondent) to the forfeiture order in the case of undue hardship.

6.15. An order for the forfeiture of property used to commit or facilitate a serious offence may also be made under a separate power in the Sentencing Act 2002, and form part of the sentence imposed on an offender. The effect of such an order is also to vest the property in the Crown absolutely.

6.16. The CPR Act confers investigative powers (in a run of provisions from s101 to s108) including as to obtaining evidence which is material to actual or contemplated forfeiture proceedings, obtaining search warrants, obtaining production orders in relation to documents, and also witness examination orders (usually directed at the obtaining of documents and other information by way of evidence).

6.17. The powers conferred on Police in the CPR Act regime are similar to those which apply to other parts of the Police when working on investigation of criminal offending. Although the proceedings under the CPR Act are very clearly intended to be civil in nature, under the High Court Rules of civil procedure, the Supreme Court has noted "substantial overlap between the purposes of the CPRA – removing economic incentives to offend and, in this way, disincentivising offending – and those of the criminal law".[37]

Asset recovery outcomes

6.18. On most accounts, the CPR Act system in the hands of enthusiastic and well-drilled Police and Prosecutor operations has been wildly successful. It is a high-profile deterrent force, countering to some extent the

[36] *Cheah v Commissioner of Police* [2020] NZCA 253.
[37] *Marwood*, above, at [19].

attractions that organised crime gangs can use, such as cars, motorbikes, boats, jet skis, flashy bling and assets, to lure new recruits. Nothing speaks as symbolically in this field of crime prevention as a fleet of criminal toys being loaded up onto a confiscation truck pursuant to a surprise freezing order operation.[38]

6.19. As at the end of October 2020, assets under restraint between the 5 regional Asset Recovery Units for the Commissioner of Police had grown to NZ$428m cumulative since July 2017. The top 3 offences used as a basis for seeking the asset restraining orders were reported by Police as being: money laundering (56%), drug crime (26%) and fraud (12%).

6.20. The largest single forfeiture to date has been a NZ$43m settlement reached in 2016-17 with a Chinese person resident in New Zealand, Mr William Yan, who was wanted for offences back in China and agreed to forfeit major property and shareholding interests in New Zealand as part of an agreed settlement.

6.21. Property that has eventually been forfeited to the Crown under the CPR Act regime (a process that can take years for all challenges and appeals and third party interests in the property to have been heard) is sold at auction or by other methods. The proceeds from that are lodged in a government Proceeds of Crime Fund administered by the Ministry of Justice. A variety of government agencies and some selected non-governmental organisations can then bid for funding for specific community or criminal justice projects they wish to carry out, such as drug treatment, healthcare services or offender rehabilitation programmes. There is a strong preference for funding initiatives at a grassroots level to fight organised criminal gang influences, especially where they are dealing in methamphetamine and other drugs.

6.22. The Asset Recovery Units/Financial Crimes Group of the NZ Police has produced a short public relations video that usefully explains to laypersons the type of work it does, and what happens to confiscated assets to recycle them and use the funds for various community benefit programmes: https://www.facebook.com/NZPolice/videos/390706962279458

6.23. In one notable case, the CPR Act legal artillery has been used against a Canadian resident named Edward Gong, already under suspicion to fraud allegations in North America, but also apparently a person who found New Zealand an attractive place to invest.[39]

6.24. Mr Gong is a Chinese national living in Canada. In 2016-17, he was being investigated by both the Economic Crime Investigation Department of the Public Security Bureau in China and the Ontario Securities Commission in Canada. The investigations concern an alleged large-scale fraud, alleged to involve a pyramid scheme associated with the sale of health supplements. It is said that his schemes gave rise to unlawful benefits exceeding $200 million, of which the authorities argue that Mr Gong remitted some $77 million obtained from the fraud to New Zealand.[40] Once the funds were in this country he used money alleged derived from the fraud to purchase property and assets in New Zealand. In 2017 the New Zealand Commissioner of Police brought a CPR Act case and obtaining orders to freeze much of the New Zealand assets. Protracted court proceedings have been on foot since.

6.25. This restraining order case ended up progressing in parallel with another proceeding which focused on the anti-money laundering breaches of a foreign exchange remittance firm used by Mr Gong (see *R v J, QF and JFL* discussed in part 8 of this report).

[38] https://www.rnz.co.nz/news/national/429854/police-make-arrests-seize-property-and-luxury-cars-in-money-laundering-probe.
[39] https://www.nzherald.co.nz/nz/canadian-xiao-hua-gong-claims-evidence-to-freeze-70m-in-nz-coerced-in-china/TTT4PSLHRW22G5IGLTON2J7P5U/.
[40] *Commissioner of Police v Gong* [2019] NZHC 2735.

7. OTHER RELEVANT MEASURES, OUTSIDE THE ANTI-MONEY LAUNDERING REGIME

7.1. This part of the report touches upon related policy developments in adjacent areas of financial/corporate regulation, property and asset investment controls. They are not, strictly speaking, part of the AML/CFT regime but help fulfil subsidiary and supporting purposes aligned with that regime. Detailed exposition of these ancillary areas is well beyond the scope of this report, so my comments are necessarily selective.

Registration systems for all financial service providers and company directors

7.2. Another important part of the financial regulatory system for the past decade involves the Financial Service Providers (Registration and Dispute Resolution) Act 2008 ("FSPR Act"), a regime to list and register all types of businesses providing financial services. This was introduced at the time, in part, to meet what is now FATF Recommendation 26, as to member nations having (at a minimum) a licencing or registration system for other types of financial institutions beyond banks.

7.3. Although it has brought some basic element of visibility to firms such as money remitters or small finance companies/lenders who were otherwise traditionally not subject to specific regulatory regimes, the FSPR Act has also encountered unexpected difficulties, and been amended many times to try to overcome those.

7.4. A key problem was that the register was never intended to be any sort of active monitoring or conduct-focused regulatory regime; as one commentator put it, this was never more than a telephone directory listing all financial services businesses. Due to those limited intentions, the register was run out of an adjacent part of our ordinary Companies Registry office, and never resourced like a proper regulatory regime. Combined with a high level of foreign ownership of such financial firms, and no clear requirement for local customers, or office presence, the registry attracted a number of foreign businesses who could be run entirely from offshore, but register for the reputational advantages of a New Zealand FSPR listing.

7.5. Some predominantly offshore-controlled entities (including fraudsters and scam artists) went further and used a FSPR listing to give their foreign client-base the mistaken impression that they are actively regulated in New Zealand when that was not the case. After a number of reforms to clamp down on this, the latest in recent March 2021 legislative amendments that radically changed parts of this Act, it has essentially led to a set of moves to migrate more businesses (such as consumer finance companies, online forex traders, and 'loan shark' lenders into different proper regulatory licensing systems. Now, capacity tests and fit or proper person tests apply, as consumer protection measures, which have improved this flawed FSPR system.

7.6. Related to that, concerns had been raised about New Zealand's company law administration, which at one time allowed a sole director to run a local company entirely from overseas. An important policy change in 2015 for the Companies Act 1993 and Limited Partnerships Act 2008 was a specific response to concerns that it has become too easy to set up and run shell companies domiciled in New Zealand. A number of dubious consultancies specialised in setting up shelf entities with only a tenuous connection to New Zealand. As a result of separate moves to clamp down on these activities, reforms now require at least one local domiciled director or agent (or an equivalent director of an Australian company. Along with the provision of more information to the Companies Registrar accordingly, and with tax evasion and offshore trust crackdowns as recommended in the *Shewan Report*, and inclusion in the AML/CFT regime as reporting entities, this step has seen fringe providers or rogue consultants largely vanish from the corporate services scene.

Context to recent changes to New Zealand's Overseas Investment regime

7.7. As a small, open trading nation, New Zealand receives a great deal of inward overseas investment, especially from Australia but in recent years also China, with whom we have a free trade agreement.

Official measures put foreign investor ownership at up to 40% of our economy.[41] New Zealand generally welcomes foreign investment, however, we have seen a rush of foreign investors into property markets, particularly in Auckland. Like Vancouver, and Sydney, and other cities offering a good quality of living, Auckland has seen a booming overheated property market, with consequent housing shortages and serious home ownership affordability problems. A variety of complex economic factors fed into that situation, but foreign investment and speculation has been one of those. Politically, calls grew for reform in our legislation and investment rules, as a move away from the previous liberal regulatory approach.

7.8. While some of the land investment was long term, some was speculation, and some involved overseas parties possibly earning money from fraud, corruption or other criminal sources. Background checks were traditionally light, the focus was on other criteria, and the regulator in form of the Overseas Investment Office ("OIO") attached to our Land Registry department was ill-equipped for deep investigations.

7.9. Accordingly, from about 2015 onwards, there have been progressive steps to tighten up our current laws covering foreign investment, especially for coastal or sensitive or residential land. The key rules are in the Overseas Investment Act 2005 ("OI Act") and the Overseas Investment Regulations 2005, amended regularly. These rules regulate significant business asset sales, residential, farmland, agriculture and fishing quota interest, but my comments and examples below focus on property investment.

Requirements under the Overseas Investment Act 2005

7.10. The OI Act 2005 sets out a regime for controlling overseas investments in sensitive New Zealand assets, as defined under the Act.[42] The legislation targets "overseas persons" which is also defined.[43] The purpose statement in the Act acknowledges that it is a privilege for overseas persons to own or control sensitive New Zealand assets, and to require that overseas investments in those assets, before being made, meet certain criteria for approval or special Ministerial consent, and impose conditions on foreign investments.[44]

7.11. The Act also has the purpose of managing certain risks, such as national security and public order risks, associated with transactions by undesirable overseas persons. The process and tests applied to consent applications for purchasing land or assets have therefore always had a political element, with the OIO having more Government Ministerial approval interventions than most impartial regulatory agencies suffer.

7.12. The most significant control features of the Act involve consent granting processes for overseas investors. Those processes have been progressively tightened, and waiting times lengthened. For example, since 16 June 2020 overseas investors have needed to notify the OIO of all investments resulting in more than 25% overseas ownership of a New Zealand business or its assets; or an increase to an existing holding up to specified higher thresholds. These notified transactions are then on hold while being assessed (aspiring to do so within 10 working days) to check they are not contrary to New Zealand national interests.[45]

7.13. Under the OI Act a transaction requires consent (under section 10(1)) if it will result in:

- an overseas investment in sensitive land; or
- an overseas investment in significant business assets.

7.14. "Transaction" is defined under the OI Act and includes:

- the sale or transfer of property or securities; and
- the issue, allotment, buyback, or cancellation of securities; and
- the arriving at, or giving of effect to, an understanding.

---

[41] LINZ, Changes to the Overseas Investment Act, as at 18 February 2021.
[42] Overseas Investment Act 2005, s 6. Overseas Investment Act 2005 No 82 (as at 22 March 2021), Public Act Contents – New Zealand Legislation.
[43] OI Act, section 7.
[44] OI Act, Section 3.
[45] LINZ, Overseas investors must continue to notify OIO, as at 2 September 2020.

Changes New Zealand has made to curb foreign investment

7.15. In 2018 the Government changed the OI Act to limit overseas purchases of residential land.[46] Although there are exceptions to this, such as for developing new land or subdivisions that will add to New Zealand's housing supply, it is extremely difficult for a non-resident to now buy a pre-existing New Zealand house. In 2019 under this policy exception to incentivise building that will ease the Auckland housing shortage, 7 one-off consents were granted for investors to develop lots for up to 240 homes, and to construct 90 new apartments.[47] Supply-side measures in the property market have therefore been abrupt, politically driven, and severe, but they have effectively curtailed overseas investors from taking advantage of booming house-price rises. This has helped in small ways, but certainly not corrected, the runaway property market

7.16. In October 2018, the coalition Government (then Labour, Greens, New Zealand First parties) required Treasury to lead a deep review of the Act and Regulations.[48] The aims of the review focused upon the OI Act's purpose "that it is a privilege for overseas persons to own or control sensitive New Zealand assets", and in particular the review claims to:

- enable the Government to effectively manage overseas investment; while
- ensure that the Act operates efficiently and effectively; and
- support overseas investment in productive assets.

7.17. Around that time, the Finance Minister announced further overseas investment rules change to include most residential and lifestyle properties.[49] Also during that period, tax policy settings have been adjusted, under what is known as a "bright-line test", that penalises investors (whether foreign or local) if they sell a house for profit, inside of 5 years of purchasing it.

7.18. Recently there has been the implementation of the Overseas Investment Amendment 2018, and the Overseas Investment (Urgent Measures) Amendment Act 2020, after Covid-19 struck.

Regulator enforcement of misconduct under the Overseas Investment Act 2005

7.19. The Chief Executive of Land Information New Zealand is the regulator appointed under s 30 to administer and supervise operation of the OI Act. In practice, the OIO is the arm that regulates overseas investment and enforces breaches, alongside other Government agencies. Over a period of about 5 years, the OIO has built up its investigative team and enforcement capability, from a low base point, to now play a larger part in the regulation of overseas criminal matters too. That was spurred by cases highlighting dubious sources of investment money, or devices to hide the actual overseas persons who were beneficial owners in some way but did not disclose that in the consent papers to the OIO to purchase property in New Zealand. The OIO enforcement team now liaises closely with the Police FIU on cases having suggestion of ML overseas.

7.20. The requirements for overseas persons to notify changes and seek consent benefits the enforcement function of the OIO, which has also undergone and overhaul and received more funding. It tackles situations where overseas people come to own or control New Zealand sensitive property previously allowed without consent, or if they did not get consent before the transaction.[50] This ensures that the OIO can keep track of overseas investors' plans, investigate whether they give truthful information and keep to any land use or other commitments they made when they applied for consent.

7.21. The courts take it increasingly seriously if an overseas person breaches the OI Act. The High Court can order pecuniary penalties for these breaches, or divestiture of the property.[51] An example was *Chief Executive of*

[46] Overseas Investment Act 2005, s 16 as amended.
[47] LINZ, OIO media release, 28 November 2019: https://www.linz.govt.nz/news/2019-11/overseas-investment-supports-housing-supply.
[48] The Treasury website, Reform of the Overseas Investment Act 2005, as at 16 October 2018.
[49] LINZ, OIO media release, 17 October 2018: Second phase of overseas investment rules review | Land Information New Zealand (LINZ).
[50] LINZ, Enforcement under the Overseas Investment Act 2005, as at 16 June 2020.
[51] Overseas Investment Act 2005, sections 47-48.

Land Information New Zealand v Tang[52] where a group of Chinese citizens not ordinarily resident in New Zealand made arrangements to purchase a residential property in Auckland for $NZ5.128 million. A standard form agreement for sale and purchase of land was used, signed by Mr Tang but with intentions he would nominate the other parties to become owners. The agreement had an option to make it conditional on consent being obtained under the OI Act, but this was not taken up. In fairly flagrant breach, no parties involved sought or obtained consent for the acquisition of an interest in property. Ultimately they agreed to settle the matter after an OIO investigation, and the High Court made orders that those in breach pay a civil pecuniary penalty. The house had, by then, been on-sold for profit so it could not be divested.

7.22. Applying a series of aggravating or mitigating factors developed by the courts when exercising their discretion on the quantum of penalty,[53] Lang J went through this exercise and ordered Mr Tang, who had bought local property before and was experienced in business matters, to pay NZ$110,500, and the other defendants who had actually profited from the house sale to each pay over $200,000.[54]

7.23. In June 2020, a solicitor was prosecuted and fined for obstructing the OIO, the first occasion an advisor had also faced enforcement action.[55] The facts were somewhat complicated but involve Dr Choi (an Auckland lawyer) who was approached by a Dr Hur to help buy a lifestyle rural property north of Auckland. Dr Hur is a Korean citizen, resident there, and deemed an overseas person under the OI Act. He entered into an unconditional sale and purchase agreement for the property for NZ$3 million.

7.24. It was claimed Dr Choi and Dr Hur obstructed the OIO during an investigation into acquisition of sensitive land. Dr Hur should have obtained consent from the OIO but did not. Instead, he engaged a different solicitor who said he should cancel the agreement and forfeit his deposit. He disregarded this advice and after unsuccessful attempts to find a mechanism to settle the property sale without further breaches, he engaged Dr Choi. That lawyer recommended the use of a company owned by his wife to settle the transaction, as a device to nominate a different purchaser of the property and provide funds to settle. The purchase was completed in 2016 in breach of the OI Act, as Dr Hur retained control and the company holding the property on his behalf acted as an associate. Hur was penalised $100,000 and Choi $60,250.[56]

Latest version of New Investor test incorporates criminality checks

7.25. Yet another version of the new investor test just came into effect on 22 March 2021, under the Overseas Investment (Urgent Measures) Amendment Act 2020. That will be a significant change for overseas applicants (it does not apply to New Zealanders). The OIO highlights that "the purpose of the new investor test is to determine whether investors are unsuitable to own or control sensitive New Zealand assets."[57] The test applies to 'relevant overseas persons' and 'individuals with control', including any corporate investors. The new test replaces the 4 parts of the existing test with 12 factors that include deeper assessment of any convictions resulting in imprisonment, penalties for tax evasion, corporate fines, and civil pecuniary penalties.[58] This is a culmination of increasing OIO expertise in tracing beneficial ownership and ascertaining likely criminal connections with the owners or purchase funding.

7.26. The intention behind that recent Urgent Measures Amendment Act 2020 was to create temporary power for the Government watchdogs to screen transactions that are not normally screened in more depth due to Covid-19 challenges. But it is expected the change in focus will become permanent.

---

[52] *Chief Executive of Land Information New Zealand v Tang* [2018] NZHC 382.
[53] Factors as identified by Edwards J in *Chief Executive of Land Information New Zealand v Carbon Conscious* [2016] NZHC 558 at [31].
[54] *Tang*, above at [39].
[55] Land Information New Zealand "Solicitor fined $60,250 for obstructing the Overseas Investment Office" as at 26 June 2020 https://www.linz.govt.nz/news/2020-06/solicitor-fined-60250-for-obstructing-overseas-investment-office.
[56] Land Information New Zealand "Criminal conviction for overseas investor who misled the Overseas Investment Office" as at 10 February 2020. https://www.linz.govt.nz/news/2020-02/criminal-conviction-for-overseas-investor-who-misled-overseas-investment-office.
[57] LINZ, New Investor Test, as of 1 March 2021. New investor test | Land Information New Zealand (LINZ).
[58] Overseas Investment (Urgent Measures) Amendment Act 2020, s 18A.

8. ENFORCEMENT ACTION FOR ANTI-MONEY LAUDERING BREACHES

8.1. AML/CFT Supervisors can elect to bring proceedings against a Reporting Entity that has breached the AML/CFT Act, through a civil claim or through criminal proceedings. They also have a raft of other regulatory options to nudge, steer, or slap Reporting Entities towards a stronger compliance path. As mentioned in Part 3 of this report, enforcement is guided by a regulatory pyramid, where the bulk of encounters with reporting entities are gentle compliance steps or warnings.

8.2. What we have seen in both Phase 1 and Phase 2 implementation is a pragmatic approach by the Supervisors, allowing something of a honeymoon period or learning curve for businesses newly-captured by the AML regime. However at some point, generally after entities have had their first 2-yearly auditing cycle under the regime, enforcement approaches will harden. It is important for AMLCOs and Senior Management in law firms to have a good appreciation of the serious enforcement artillery that the DIA has potentially at its disposal.

8.3. The new AML/CFT legislation in 2009 was intended to bring about a much tougher set of sanctions for non-compliance than the predecessor law. As the High Court has confirmed:[59]

- the AML/CFT Act "constitutes a significant step up in the regulatory framework" (at [20]);
- further, the maximum penalties "are 20 times greater than the fines for the equivalent breaches under the FTRA", signalling "significantly larger penalties than were formerly available, in order to effectively achieve the Act's objectives" (at [99]).

Range of possible sanctions for breach of AML laws

8.4. Part 3 of the AML/CFT Act covers enforcement, containing general provisions, civil liability and offences. There are a mix of enforcement sanctions with differing levels of potential penalty outcomes, depending on the factual circumstances and the attitude of the Supervisor to the transgression. Regulators can consider legal action for civil liability acts and also for criminal offences but not both at once.[60] Enforcement proceedings can be potentially taken against senior managers and individuals within corporate entities as well as the corporation/entity.

8.5. Civil liability acts are set out in s78 in a two-tiered penalty structure, and include:

- Inadequate account and transaction monitoring (s 78(b)).
- Entering or continuing a business relationship without adequate evidence of identity (s 78(c)).
- Entering or continuing a correspondent banking relationship with a shell bank (s 78(d)).
- Failing to ensure branches and subsidiary businesses comply with AML/CFT requirements (s 78(g)).

8.6. Statutory maximum pecuniary penalties for those civil liability acts are set at NZ$100,000 for individuals or $1 million for bodies corporate (under s 90(2)).

8.7. The following civil liability acts are also specified in s 78 with a higher penalty, reflecting the greater potential for money laundering risk:

- Failing to carry out CDD (s 78(a)).
- Failing to report transactions (s 78(da)).
- Failing to keep records as required (s 78(e)).
- Failing to establish, implement or maintain an AML/CFT compliance programme (s 78(f)).

[59] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd* [2017] NZHC 2363, [2018] 2 NZLR 552.
[60] See ss 73 – 74 of the AML/CFT Act.

8.8. For these types of compliance failings, statutory maximum penalties are set at NZ$200,000 for individuals or $2 million for corporate bodies (under s 90(3)).

8.9. Additional catch-all statutory wording allows for civil liability acts include failing to comply with any other of the AML/CFT requirements. For instance, in an early case the High Court had to examine a failure to report a suspicious transaction with unspecified penalty, and decided to follow the amounts set out in s 90(3), which are set at $200,000 for individuals or $2 million for corporate bodies as a "notional ceiling on the penalty" or "practical guideline" in the absence of legislated specific amounts.[61]

8.10. Where a civil liability act is alleged to have occurred, the court can determine a pecuniary penalty imposed under section 90 of the Act. A pecuniary penalty is a legislative device that imposes monetary penalties on a defendant after a civil trial has been conducted, often described as a regulatory hybrid of civil/criminal penalty. This penalty can be very substantial but neither imprisonment nor criminal conviction can result.[62]

8.11. As part of a gradual ramping-up of enforcement activity, the Supervisors have made liberal use of settlement actions (avoiding court proceedings) where they elect to issue a formal warning or accept a court-enforceable undertaking from the Reporting Entity.

8.12. Publicity and media attention is also an important item in the regulatory toolkit. There have been a growing number of such formal warning actions made public, although there are also many more that have not been published by the Supervisors. It can greatly escalate the severity of the situation for a Reporting Entity on the receiving end. In practice, advising a wide variety of businesses, I have seen that reputational damage (corporate, and personal to the managers) is often as much of a powerful motivating factor as the threat of financial penalties or law-suits.

8.13. For Phase 2 entities, we are at the point where after, initially at least, the Supervisors make use of warnings and enforceable undertakings rather than punitive court action, except in the most egregious of cases, there is now a noticeable hardening of enforcement approach. No reputable law firm will want to face the publicity, costs and stigma of being publicly criticised for failing in the new and onerous field of legal compliance with AML/CFT.

Criminal law culpability exists as well as civil liability

8.14. Criminal offences for breaches of the regulatory regime are set out in ss 91 -97 of the AML/CFT Act. This can include where a Reporting Entity has committed any of the civil liability acts listed above, if it does so knowingly or recklessly. That introduces a recognisable *mens rea* standard, and might be suitable if, for example, an entity breaches perhaps repeatedly or after receiving a warning from its Supervisor.

8.15. Other specific offences include:

- Recklessly, knowingly, or repeatedly carrying out a civil liability act as above (s 91).
- Failing to make SARs when required (s 92).
- Providing false or misleading information concerning SARs (s 93).
- Tipping off unauthorised third parties about SARs or PTRs (s 94).
- Failing to keep adequate records concerning SARs (s 95).
- Obstructing a SAR or PTR investigation (s 96).
- Failing to make PTRs when required (s 97).
- Disclosing in any judicial proceeding information contained in a SAR unless exceptions apply (s 97).

8.16. For these more serious matters, the maximum sanction under s 100 is a criminal fine of up to NZ$300,000 or up to 2 years' imprisonment for individuals, or fine of up to $5 million for corporate bodies.

---

[61] *Ping An Finance* (above) at [86].

[62] New Zealand Law Commission report, *Pecuniary Penalties*, August 2014, at 4.

8.17. There are also offence provisions relating to the cross-border transportation of cash by any person, whether a Reporting Entity or not, which are typically enforced by NZ Customs at airports and border controls. These are considered more minor offences and have a maximum penalty under s 112 of a term of imprisonment of not more than 3 months and/or a fine of up to $10,000 for an individual or a fine of up to $50,000 for a body corporate. These provisions came into effect prior to the main AML/CFT Act compliance obligations, and resulted in the first prosecutions under the AML/CFT Act brought by the Customs Service. Those were based on the non-declaration of large sums of cash movements by people passing through New Zealand's border control stations.

8.18. If the Supervisor chooses to proceed by seeking a civil pecuniary penalty, the ordinary High Court Rules apply as to the usual civil procedure. The balance of probabilities civil onus of proof applies. In those cases, a standard civil limitation period will apply. An application to the High Court must be made within 6 years of the conduct that gives rise to the liability to pay the civil penalty (s 72 of the AML/CFT Act).

8.19. When a Supervisor moves to bring criminal charges, the time limit for the majority of regulatory offences under the AML/CFT Act is 3 years "after the date on which the offence was committed".[63] For the more minor or summary offences relating to the cross-border transportation of cash, the time limit for initiating a charging document is 6 months after the date on which the offence was committed.

Potential for civil claims, and some immunity from suit

8.20. The field of private claims or civil liability for AML breaches is very underdeveloped in New Zealand. In relation to civil liability acts under the new AML regime, the primary right and responsibility to take action rests with the AML/CFT Supervisor, and the civil "balance of probabilities" onus of proof applies. However, if a pecuniary penalty is sought, the Court has the ability to order it to be paid to the Crown "or to any other person specified by the court" under s 90(1), which could allow payment to be directed to victims of crime or others affected.

8.21. In practice, the usual court order is a payment to the Crown, similar to a fine. However, as part of the criminal process, victims who can show an effect may seek reparation payments or courts can order that part of the fine be paid to victims. As the enhanced AML regime matures, and as the financial consequences become more serious for Reporting Entities in future, more civil lawsuit problems are likely.

8.22. Reporting entities have a form of statutory immunity from civil suit for actions taken to comply with the AML/CFT Act, so long as they were acting in good faith and reasonably (see s 77). For plain cases of non-compliance or breach where no attention or reasonable care was taken, potential common law causes of action may remain available, such as equitable tracing remedies, claims of knowing assistance or knowing receipt of property from the proceeds of crime, breach of 'bankers' mandate; fraud or breach of trust or even the tort of breach of statutory duty.

8.23. At a practical level, increasing use by the Crown of the Criminal Proceeds (Recovery) Act 2009 regime tends to preclude or "crowd out" the likelihood of private claims by victims, because the Crown usually targets those assets of an offender with the most realistic prospect of realising value, frequently leaving few viable assets for a private claimant. For those with an interest in civil asset forfeiture and restorative justice to victims, that is not necessarily a good outcome.

8.24. Notably, however, Australia has a much more developed class action litigation landscape, affecting banks found to be in breach. After the Commonwealth Bank of Australia (CBA), parent of large New Zealand bank ASB, ended up paying an unprecedented AUD 700 million penalty to the Australian regulator in 2018 (see below) it now faces civil class action suits. That may be a growing factor in New Zealand in future.

[63] See ss 99 and 104 of the AML/CFT Act.

Limited case law guidance so far, but does highlights hefty penalties

8.25. So far the DIA has been by far the most active in court of the three AML/CFT Supervisors. To date, it has brought enforcement action under the AML/CFT regime in 2 criminal prosecutions of a reporting entity (and related individuals who ran it), and also in 4 cases seeking civil pecuniary penalty. It has obtained judgment in 5 of those cases at the time of writing. One is currently still under appeal, and another only recently commenced.

8.26. However, this might be considered at this time still a very limited body of case-law because all of the civil action cases to date have been effectively settled prior to the Court outcome, or determined with liability agreed and only quantum of penalty disputed. In several cases the defendant business has not taken steps to defend the case, due to lack of funds or imminent insolvency, so only submissions from the prosecutor have been heard. These 4 cases are summarised below:

- Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd [2017] NZHC 2363;
- Department of Internal Affairs v Qian DuoDuo Ltd [2018] NZHC 1887;
- Department of Internal Affairs v Jin Yuan Finance Ltd [2019] NZHC 2510;
- Department of Internal Affairs v MSI Group Ltd & OTT Trading Ltd [2020] NZHC 1005.

8.27. The first two of those cases commenced at the same time, arising out of inter-related DIA investigations but then proceeded down divergent court paths, resulting in very different penalty outcomes.

DIA v Ping An Finance (Group) NZ Company Ltd, and Xiaolan Xiao [2017] NZHC 2363

8.28. Ping An was a New Zealand incorporated company that has carried on business providing money remittance and foreign currency services. It serviced almost exclusively an Asian language community. Between 1 January and 9 January 2015, Ping An was alleged to have committed numerous civil liability acts, in that the company:[64]

1) failed to carry out customer identity and verification of identity checks as part of customer due diligence;
2) failed to adequately monitor accounts and transactions;
3) entered into or continued business relationships with persons who did not produce or provide satisfactory evidence of their identity;
4) failed to keep transaction, customer due diligence, and other records; and
5) failed to report suspicious transactions in breach of requirements in Part 2 of the Act.

8.29. Toogood J regarded these breaches as "serious and systematic deficiencies in complying with a multiplicity of obligations under the Act".[65] He also found that the sole director/shareholder of Ping An had misled DIA in the course of its investigation and demonstrated a complete disregard for the Act's requirements. In this judgment, Toogood J determined that any pecuniary penalty imposed under the Act must be so significant as to deter and denounce non-compliance.[66] Injunctions were also granted restraining Ping An and Mr Xiao from carrying out financial activities.

8.30. Like the *Jin Yuan Finance* case that followed later (but not connected, see below), the *Ping An Finance* case involved defendants who were a money-remitter company and its sole director/proprietor, but who did not make an appearance at the hearing. So those cases were effectively an undefended, default-type hearing upon formal proof, and some caution might be necessary accordingly. Despite that, the High Court in *Ping An Finance* took the opportunity to make comments on important aspects of the new regime as it was the first time enforcement action against a reporting entity had come to the High Court.

---

[64] *DIA v Ping An Finance (Group) NZ Company Ltd, and XiaoIn Xiao* [2017] NZHC 2363 at [5]; altern. [2018] 2 NZLR 552.
[65] *Ping An Finance* (above) at [6].
[66] *Ping An Finance* (above) at [8].

8.31. Toogood J held that Ping An Finance had, on the balance of probabilities, committed the 5 civil liability acts on multiple occasions and ordered it to pay a total of $5.29 million in pecuniary penalties. That is a very large penalty, in New Zealand norms, at least for a brand-new regulatory regime straight out of the box.

8.32. Subsequent to the *Ping An Finance* decision a fair bit of action took place. The director of Ping An Finance was convicted of money laundering in a separate criminal case; but then belatedly decided to take steps to challenge matters. He sought (unsuccessfully) to have the formal proof judgment set aside; and a bankruptcy notice was issued against him by the DIA on the basis of the unpaid costs award of $44,850. The company itself was also put into liquidation. Its director Mr Xiao then attempted to appeal to the Court of Appeal, acting in person, on grounds of procedural irregularity.

8.33. Those efforts failed, with the Court of Appeal eventually saying:[67]

> "[41] …We accept that pecuniary penalties may be punitive in substance. Those imposed under the AML/CFT are imposed primarily for the purposes of deterrence and denunciation. That does not, however, mean that different procedural rules should apply to such claims as opposed to other forms of civil proceedings.
> [42] A defendant who fails to take steps to defend a proceeding will have been served with a statement of claim that satisfies the pleading requirements set out in pt 5 sub-pt 4 of the High Court Rules, including identifying the distinct causes of action and facts relied on for it and specifying the relief sought. A defendant served with proceedings brought under the AML/CFT Act is taken to know that pecuniary penalties of up to $1 million and $2 million for each civil liability act could be imposed."

8.34. Mr Xiao was subsequently declared bankrupt, as the DIA sought to pursue payment of the penalty.

DIA v Qian DuoDuo Ltd/Lidong Foreign Exchange [2018] NZHC 1887

8.35. The defendant Qian DuoDuo Limited ("QDD") was another money remitter company. Like many in its sector trading, it was in difficult practical trading circumstances with mainstream banks having withdrawn or threatened to withdraw access to bank accounts (a process known as "de-risking" or "de-banking"). From early 2015, the DIA established that the defendant had breached its obligations under the AML/CFT Act by virtue of failures:[68]

1) in respect of accurate and updated risk assessments
2) undertake Enhanced Customer Due Diligence
3) to undertake ongoing Customer Due Diligence and account monitoring
4) to keep adequate records.

8.36. Qian DuoDuo Limited was ordered to pay NZ$365,000 in pecuniary penalties, even thought the DIA argued there were more than NZ$100 million in transactions that had not been checked under AML CDD requirements. This was significantly less than the penalties ordered in *Ping An.* However, a wide variety of potential mitigating factors could be argued in the QDD case, which was not an undefended proof only hearing as in the *Ping An* case.

8.37. The case illustrated the complexity of the AML/CFT Act and a widespread misunderstanding of compliance obligations as to beneficial ownership and customer relationships. Powell J in concluding his judgment said, "*…in particular my assessment that the civil liability acts have not had any substantive effect on New Zealand's financial system, I conclude the conduct reflected in the four civil liability acts does not require the imposition of a significant deterrent penalty on QDD*".[69] The Court found that the defendant's failures stood at the lower end of non-compliance.

[67] *Xiao v DIA* [2019] NZCA 326.
[68] *DIA v Qian DuoDuo Ltd/Lidong Foreign Exchange* [2018] NZHC 1887 at [3].
[69] *Qian DuoDuo Ltd* above, at [144].

8.38. QDD had lower levels of culpability in part on the basis that it had tried to be compliant and had relied on external consultants' advice as to AML matters. Consultants had indicated it was compliant, and there was also a DIA desk-based review of its activities that earlier suggested it was compliant. This was reflected in the Court's adjusted starting point for a penalty of NZ$420,000, compared to a starting point of $2.6 million sought by the DIA.

8.39. The DIA allegations of breaching the AML/CFT Act in respect of QDD's risk assessment, Enhanced CDD, ongoing CDD and account monitoring, and failure to keep adequate records, all carried some degree of overlap on the facts with steps actually taken (or not taken) in the business. In order to avoid an element of double-penalising QDD for the same conduct, an original starting point of $620,000 was reduced by $200,000. Under s 74(2) of the AML/CFT Act, while civil penalty proceedings may be brought for more than one civil penalty, the person "may not be required to pay more than 1 civil penalty in respect of the same or substantially the same conduct". It was recognised that QDD's failures with respect to its risk assessment overlapped in substance with failures in other aspects of the separate breaches alleged in the pleading.

8.40. The DIA did achieve an uplift in the penalty on account of QDD's misleading behaviour once a DIA investigation was on foot. A small $25,000 uplift was given, taking into consideration that the behaviour did not affect the extent of the civil liability acts committed by QDD. The Court then allowed a 20% further discount to cover QDD's admission of liability, cooperation and subsequent steps to ensure compliance. This brought the final penalty down to $356,000, plus costs.

DIA v Jin Yuan Finance Ltd, Rex Young [2019] NZHC 2510

8.41. This was yet another case brought by the DIA against a money remitter, one dealing largely in business transactions not in the English language, with an immigrant community client base. The DIA clearly considers small and informal money remittance sector firms as high risk, although in some of these cases it might be suggested it has been pursuing "low hanging fruit" in terms of regulatory enforcement actions.

8.42. It was also undefended, after initial counsel appearing in court for Jin Yuan Finance Ltd ("JYFL") was given leave to withdraw, and it then proceeded by way of formal proof and prosecutor submissions only.

8.43. The DIA sought over NZ$4 million in penalties against the defendant company and its local director. Their claims were based on a history of non-compliance under the AML/CFT Act between 2013 and 2017. The defendant business was said to have committed civil liability acts in 6 different ways:

1) It failed to conduct customer due diligence as required by sub-part 1 of Part 2 of the Act.[70]
2) It failed to adequately monitor accounts and transactions.[71]
3) It entered into and continued business relationships with customers who did not produce or provide satisfactory evidence of their identities.[72]
4) It failed to comply with the requirement to report suspicious transactions.[73]
5) It failed to keep records as required by sub-part 3 of Part 2 of the Act.[74]
6) It failed to implement or maintain a compliance programme (sub-part 4 of Part 2 of the Act).

8.44. The DIA submitted that the defendants conduct "created a real avenue for money laundering or the financing of terrorism to have occurred in New Zealand and that the case is highly analogous to *Ping An".*[75] Woolford J agreed with the DIA and found that the breaches were at the higher end of non-compliance with the Act's requirements. He ordered the defendant to pay a pecuniary penalty of $4,007,750.

[70] Anti-Money Laundering and Countering Financing of Terrorism Act 2009, s 90(3).
[71] Section 90(2).
[72] Section 90(2).
[73] Section 90(3).
[74] Section 90(3).
[75] *Qian DuoDuo Ltd* above, at [37].

8.45. JYFL had a history of non-compliance with the AML/CFT Act between June 2013 and June 2017. The DIA issued and published a formal warning against JYFL in 2015. For most reporting entities, a public warning should be a shot across the bows in the strongest of terms that it needs to substantially improve its state of compliance. However, later DIA monitoring contact found there were continuing compliance issues.

8.46. In April 2018, restraining orders were issued against JYFL and its director, Mr Young, restraining them from carrying out any financial activities. A particular aggravating feature was that, throughout its correspondence with the DIA, JYFL had repeatedly told the DIA it was carrying out its business through one company bank account. JYFL had declared itself to have undertaken 55,097 transactions with a total of $278.5 million of business. However, it later emerged the company was in fact using 17 bank accounts. That was, in reality, a response again to de-riskng by mainstream banks. But from that JYFL's actual business was inferred by the DIA, and the Court, to be significantly greater than had been declared.

8.47. This failure to accurately describe the situation in its risk assessment and compliance documents and to the DIA was considered misleading behaviour by JYFL. That was treated as an aggravating factor by the Court.

DIA v MSI Group Ltd, OTT Trading Group LTD, and T/ QI, L.C Woon, Y. Duan [2020] NZHC 1005

8.48. The most recent case, again involving money remittance and foreign exchange businesses, resulting in further large pecuniary penalties being ordered.

8.49. A first/interim judgment confirmed a set of restraining orders against the individuals, including the compliance officer of the MSI Group. On 15 May 2020, Lang J imposed orders on the three defendants preventing them acting as senior managers or compliance officers of a reporting entity for 3 years or, in one case, indefinitely. This development tends to confirm the regulator's increasingly apparent strategy to pursue both the corporate entity for large fines, but also key individual human beings actually running the business. This outcome arose particularly from the admitted facts that the three individuals were said to have misled the DIA during investigations, including by creation of false documents.[76]

8.50. A second (undefended) judgment on 10 July 2020 confirmed hefty monetary penalties of NZ$3.1m against OTT Trading, and $4.485m against MSI Group, plus costs.77 The parties were related, and appeared to have basically no working AML compliance programmes at all, with the High Court saying "*OTT consistently failed to meet the requirements of the Act. The failures were throughout almost every aspect of the AML/CFT regime.*" OTT had previously received a formal warning from the DIA.

8.51. A restraining injunction against OTT not to carry out any financial activities that would cause it to be a "reporting entity" under the AML/CFT Act was additionally granted. MSI was already out of business, presumably insolvent, or else would have met the same injunctive fate.

8.52. This case represents the first time that an employed compliance officer, not a shareholder/director of the reporting entity, has been personally sued by the DIA.

Two high profile criminal prosecutions

R v Qiang Fu, Fuqim Che & Jiaxin Finance Ltd [2020] NZHC 366

8.53. The first criminal prosecution for breach of the AML/CFT Act was *R v QF, FC and JFL*.[78] After defended trial, convictions were entered against a company Jiaxin Finance Ltd, and 2 individuals involved in running it. Jiaxin was (again) a money remitter and currency exchange business.

---

[76] *DIA v MSI Group Ltd, OTT Trading Group LTD, and T/ Qi, L.C Woon, Y. Duan* [2020] NZHC 1005 at [6].

[77] *DIA v MSI Group Ltd, OTT Trading Group LTD, and Qi, Woon, Duan* [2020] NZHC 1663.

[78] [2019] NZHC 3058 (under name suppression at that time) as to verdicts and reasons, later *R v Jiaxin Finance Limited* [2020] NZHC 366 as to sentencing.

8.54. Also charged were the sole director of the company, Mr Fu, and his mother, Ms Che, whose degree of involvement with the business was disputed. Jiaxin, Mr Fu and Ms Che were all found liable for representative charges of:[79]

1) failing to conduct customer due diligence
2) failing to keep adequate records relating to a suspicious transaction and
3) failing to report a suspicious transaction.

8.55. Ms Che was additionally found guilty for one charge of "structuring" a transaction to avoid AML/CFT requirements. She had made 14 separate cash deposits into Mr A's bank account over four days totalling $710,772, designed to work around likely reporting thresholds. The case includes a number of interesting comments about the nature of structuring issues when breaking up transactions and chains of transactions.

8.56. The company faced 3 charges: failing to conduct CDD; failing to report a suspicious transaction; and failing to keep or retain accurate records relating to a suspicious transaction in relation to a particular wealthy customer, later reported to be Mr Edward Gong, whose New Zealand assets face CPR Act restraint (as mentioned in part 6 of this report above). The charges related to some 311 transactions with a combined value of around $53 million. All of those transactions were undertaken on behalf of that one individual customer. He allegedly operated an illegal Chinese pyramid scheme and fraudulent affairs overseas, and was suspected to have laundered the money to buy safe assets through New Zealand remitter accounts.

8.57. Ms Che had acted as the middleman between Mr Gong and the company Jiaxin. The Crown case was that this was an arrangement made to avoid CDD or ECDD being conducted on Mr Gong. Rather than treat him as the customer, Jiaxin had instead treated Ms Che as the end customer, who Jiaxin argued operated in her own right independently and not acting on behalf of another.

8.58. In sentencing, Walker J decided to impose fines of NZ$180,000 on Mr Fu, $202,000 on Ms Che and $2.55 million on Jiaxin. The case is now going on appeal, and as yet an appellate hearing date is not confirmed.

8.59. This case highlights the importance of understanding and clarifying who the customer is for AML/CFT purposes. A core CDD issue for a reporting entity is to understand whether the person it is dealing with is the end-customer or are they are acting on behalf of someone else? And what is the nature of that end-customer's business and source of funding? If unable to correctly identify its true customer then an entity is unlikely to have met its CDD obligations. The Court arguments suggested that Ms Che and her son knew quite what they were doing, and what their biggest customer Mr Gong from Canada was accused of, but they were prepared to adopt devices to avoid CDD requirements upon a lucrative customer.

R v Daniels and Simpson [2020] NZHC 275

8.60. Although not a case of prosecution by the DIA for breach of the AML/CFT Act regulatory regime, it is impossible to ignore the significance of the recent prosecution by NZ Police and jail sentence for a practising lawyer found guilty of criminal money laundering for a gang leader client.

8.61. The lawyer, Mr Simpson, pleaded guilty to 13 counts of money laundering charges under the Crimes Act, s 243(2), in acting as solicitor for Mr Daniels who was vice-president of the Comancheros organised crime/motorcycle gang. The offending involved transactions including $2m lodged with the trust account of Simpson's West Auckland law firm and then used to purchase property and other assets for Daniels.

8.62. Mr Simpson was sentenced to 2 years, 9 months imprisonment, with Van Bohemen J saying at sentencing:

> "[46] In your own words, you turned a blind eye to the source of the funds. I am satisfied that in so doing you were reckless not just to the possibility that the funds came from activities such as tax avoidance or gambling but also to the possibility that they came from much more serious offending, including drug

[79] *R v Jiaxin Finance Ltd* [2020] NZHC 366; [2020] NZCCLR 18 at [1].

> offending. The amounts and numbers of transactions themselves ought to have put you on notice. And yet you chose to continue, regardless of that possibility, as indeed you did once you had made your inquiries in November 2018. I am satisfied that you were at least reckless for the whole of the period of the offending and probably more than that after you had made your inquiries.
>
> [47] In addition, you were acting in your professional capacity and when you chose to continue your involvement, even when your suspicions were raised, you not only placed your personal gain above your duties as a lawyer but you risked bringing your profession into disrepute. That is a significant distinguishing factor."

8.63. It appears the transactional work and solicitor's retainer period in issue in the case continued through the period after 1 July 2018 when lawyers first became subject to the AML/CFT regulatory regime. Although not commented upon in the decision, it appears almost certain the factual scenario meant that Mr Simpson would have also been in breach of a number of AML/CFT regulatory obligations concerning his gang member client. Of course, charges for money laundering under the Crimes Act with a maximum penalty of 7 years jail per offence, reflected the far more serious element of the misconduct.

8.64. There can be no doubt that the High Court cases so far are treating AML breaches as very serious in terms of likely penalty outcomes. The judiciary may well tend to see lawyers in the harshest light (given a lawyer's level of professional knowledge and ethical responsibilities) when they come before the courts in future for sanctions under the AML/CFT Act 2009, let alone the Crimes Act for actual laundering.

8.65. In the Court sentencing notes, it was noted that much of the funds into trust account probably derived from drug dealing activity, and that the legal fees made by Mr Simpson were probably modest. The money laundering of 13 transactions came to a value of almost NZ$3.3 million. Some of this money also benefited Mr Daniels and gang affiliates directly as he purchased three luxury vehicles.

Banking sector action limited, while overseas penalties for AML breaches grow enormous

8.66. For Phase 2 reporting entities, there have been a number of early compliance engagements with the DIA resulting in private non-published warnings, but no matters yet commenced in Court. However, the situation is very recently moving towards a tougher enforcement settings, as in March 2021 the DIA released details of the first public warnings issued against a real estate agency firm,[80] and a law firm.[81]

8.67. Compared to the DIA, the other Supervisors have not been nearly as active in enforcement. That might partly be a function of resourcing and priorities, as both the FMA and the RBNZ have a lot of other non-AML regulatory and licensing responsibilities in handling banking, life insurance, superannuation, wealth management and financial advisory firms.

8.68. However, in the case of the Reserve Bank, the question can be posed whether it is institutionally conflicted in being tasked with acting as a strong enforcement action body for large banks? It has a number of mixed policy objectives laid down by government, including macro-economic market stability, monetary policy and other policy levers on issues such as an overheated housing market, that are an ongoing challenge where the cooperation and input of major mortgage lending banks is necessary. A small team of AML regulation specialists also sitting within the RBNZ might find their good work somewhat diluted or overwhelmed by other competing central bank priorities.

8.69. The FMA has only recently in 2020 commenced its first civil enforcement claim to Court, against a forex/derivatives broker trading business. The RBNZ is following suit with a New Zealand domestic bank, reportedly in protracted negotiations (and engaging in a large expensive remediation programme to

[80] https://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/3f2353eeb9b0a20ecc25868a0080f114!OpenDocument.
[81] https://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/e658d7c8d70b8280cc25869a007eac10!OpenDocument.

correct past AML account failings). Whether that results in any court outcome or simply a negotiated settlement or warning remains to be seen, and so far details from the RBNZ itself are scant.

8.70. In Australia, the singular AML-focused regulator there (AUSTRAC) has taken some very large cases to Court against large reporting entities, with more in the pipeline. This includes a trio of ground-breaking civil enforcement cases, each with spectacularly large agreed penalty outcomes:

- TabCorp, a major casino and gambling firm, for compliance failures resulting in agreed penalties of AUD 45 million.[82]
- Commonwealth Bank of Australia (CBA), for a raft of compliance failings that allegedly facilitated actual cash money laundering through many transactions using new "intelligent deposit" technology implemented in bank branch ATMs, resulting in a massive AUD 700 million agreed penalty.[83]
- Westpac Banking Corporation, for what the regulator says was a "longstanding and systemic failure … to comply with its legislative obligations" in potentially contravening the Australian equivalent AML/CTF Act 2006 on over 23 million occasions, including international funds remittance transactions that allegedly facilitated online child abuse activities carried out in the Philippines. The case eventually reached an agreed penalty position, approved by the Federal Court as a whopping AUD 1.3 billion civil penalty, significantly eclipsing even the massive CBA penalty.[84]

8.71. To some extent, because those two banks each have local New Zealand subsidiary banks, and our financial sectors are deeply intertwined with those in near-neighbour Australia, the RBNZ may be getting some spillover benefit from those cases. Local banks are in effect now lifting their compliance game in New Zealand, in the shadow of the very heavy crackdown on AML/CFT breaches that has occurred in Australia.

Non-financial penalties

8.72. The High Court can also grant injunctions and certain types of non-financial penalties. Injunctive orders were made, for instance, in the Ping An Finance case preventing that company and its director Mr Xiao from carrying out any financial activities that would cause either of them to be a "financial institution" under the AML/CFT Act. The same orders were sought by the DIA and granted against Jin Yuan Finance Ltd and its director Mr Young.

8.73. These cases are making clear the Court's willingness to not only impose significant pecuniary penalties in order to deter and denounce non-compliance, but also to remove from errant individuals their ability to work in the regulated sector in future.

8.74. Orders banning a person taking a director role in a company are also possible. For a banking executive or law firm partner that could be catastrophic. Personal accountability for a business's compliance with the AML regulatory regime is clearly something that will be taken very seriously by the courts.

[82] *Chief Executive Officer of Australian Transaction Reports and Analysis Centre v TAB Ltd (No 3)* [2017] FCA 1296.
[83] *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited* [2018] FCA 930.
[84] *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Westpac Banking Corporation* [2020] FCA 1538.

9. BALANCING PRIVACY RIGHTS AND INFORMATION-SHARING CONSIDERATIONS

9.1. Viewed at a high level, much of the AML compliance complexity can be seen as boiling down to data management issues. Reporting entities must obtain much greater data from (and about) customers than previously required, then corroborate it in more depth, retain records that can be reconstructed quickly (even years later) and also assemble and pass on information to the NZ Police in the form of statutory reporting processes.

9.2. With such vast rivers of sensitive personal information flowing around, data protection and cyber-risk concerns are very real.

9.3. Privacy law considerations must be balanced with the AML/CFT Act obligations, even if the two represent a sometimes uneasy tension for regulated businesses. There is a similarity in these broadly conflicting policy goals to the legal professional privilege tensions explored in part 5 of this report, for lawyers. However, unlike the privilege debate, where the conflict becomes irreconcilable it is generally the privacy and personal data protection rules that Parliament has determined should give way, if necessary, subservient to the financial crime prevention policy goals.

9.4. Entities under the AML/CFT Act must have regard to privacy issues and protect the personal information they collect and hold. This is expressly required in certain parts of the AML regime, such as in relation to the sharing of information among members of a designated business group ("DBG") in order to pool resource and spread the work of the compliance burden.

9.5. Privacy is also an important consideration under the Amended Identity Verification Code of Practice 2013, jointly issued by the AML/CFT Supervisors to guide entities on ways to verify the identity of new customers and the owners/representatives of those customers.

9.6. This concluding part of my report briefly examines three aspects of information management and data-sharing within the AML regime:

- Avenues where reporting entities are permitted to share information with one another for AML/CFT purposes;
- How the Police FIU receives and utilises information provided by reporting entities;
- Privacy law principles interposed with the AML regime, and the views of the Office of the Privacy Commissioner.

Reporting entities may rely on third parties/agents/affiliates for compliance functions

9.7. One of the unfortunate elements of the CDD (or KYC) requirements in the AML regime is that multiple reporting entities end up requesting the same data from a client and having to verify it. In some scenarios a bank, lawyer, financial advisor and/or accountant may each end up having to ask the poor client the same questions. As a result, there can be duplication and inconsistency in the process. To some extent this is unavoidable. But to reduce administration work and transaction costs for these parties, the AML/CFT Act makes some concessions allowing entities to make arrangements for reliance on each other, or on third parties/agents for KYC checks and other functions.

9.8. For that to operate, at some level information sharing must be part of the arrangements, and this could impinge on a person's reasonable expectations of privacy.

9.9. The AML/CFT Act has a series of provisions (ss 32 – 34) permitting entities to rely on other parties to help do some of the KYC work for them. These provisions are merely enabling mechanisms, if firms choose to set up arrangements to take advantage of them, not legal requirements.

9.10. The most common way in which entities choose to make use of the "reliance on other entities" avenues is to establish a designated business group. As mentioned earlier, this DBG concept is available to entities and groups of entities that are related or connected in some ways. It is a compliance construct, not a legal entity or corporate form, to enable some AML/CFT functions to be jointly resourced and for sharing compliance responsibilities.

9.11. AML/CFT Supervisors jointly issued a set of DBG Formation and Scope Guidelines,[85] which explain how entities can form or join a DBG, and then one member of a DBG can rely on another member to carry out some obligations on their behalf. These include potentially sharing:

- Initial CDD or onboarding for new customers;
- parts of an AML/CFT programme — such as record keeping, account monitoring and ongoing CDD;
- annual reports to be submitted on behalf of another member of the DBG;
- Risk Assessment documents, provided that the members share similar risks and address any that are different;
- the role of the AML Compliance Officer;
- managing the process of suspicious activity reporting; and
- joint prescribed transaction reporting.

9.12. Section 32(1) of the Act sets out the key features of these shared functions. For Member A to rely on another Member B to do CDD, conditions in s 32(1)(a) require that customer identity information must be passed on to Member A who needs it *before* establishing the client relationship; and verification of the ID data must be passed upon request as soon as practicable or at least within 5 working days of the request.

9.13. A specific privacy control provision exists in s 36 of the Act for DBG members who pass customer information around in this way. It requires, in essence, each member to apply equivalent privacy protection mechanisms to the data, to use and disclose it only for limited purpose and, if one of the members is overseas, to agree in writing that equivalent privacy protections in that country will apply.

9.14. Only if a group of businesses have the eligibility to structure themselves this way (e.g. if related companies or under ultimate shared ownership) will a DBG assist. DBG eligibility options can be limited for some entities, such as an alliance of separately owned law firms. So the assistance enabled by s 32 is sometimes limited in scope for many reporting entities.

9.15. Sections 33 and 34 of the Act have possibly more utility for firms contemplating how they can rely on other parties for CDD procedures — although these avenues also come with strings attached. In simplified form,[86] the effect is that some reliance may be possible in situations where a reporting entity is:

- dealing with another New Zealand Reporting Entity;
- dealing with a person overseas who is an equivalent reporting entity there, supervised/regulated for AML/CFT purposes in another country that is considered to have sufficient AML systems and measures in place;
- arranging to appoint a third party to act as its direct agent.

9.16. Appointing an agent to carry out CDD is superficially attractive, but given the potential liability risk it entails, in practice there have not been a great many such arrangements reached. The concept of an agent is undefined for specific AML purposes, and so ordinary common law principles of agency will apply. This probably enables a wider scope for a person if suitable and willing to be authorised to do CDD and pass

[85] DBG Formation and Change Guideline, as at February 2020 DBG-formation-and-change-guideline-2020.pdf (fma.govt.nz).

[86] Potentially, 2 other forms of reliance exist – one intended to create a series of "Approved Entities" upon which an entity could rely if the Ministry so declares (but to date no such Approved Entities yet exist); and another mechanism in the "Managing Intermediaries Class Exemption" which does exist, but is so convoluted and narrow in it terms that in practice many entities have chosen not to use it.

information on for the reporting entity to discharge its AML obligations. But while the agent is the person who obtain that information, and usually perform the verification of it, everything is done on behalf of and in the name of the principal, and all data must be properly procured and sent in full at the times required.

9.17. In the event, uptake of these enabling provisions has been low in New Zealand, so they have not delivered the usefulness originally hoped. The key challenge is that, where an entity outsources some of their compliance work to others, the entity remains liable under the Act if something goes wrong or the third party does not correctly discharge the CDD function. That means the business could still face potential sanctions for breach of the AML/CFT Act - which it cannot contract out of (see s 9) – and would be left having to attempt civil law recovery via negligence claims or perhaps a contractual indemnity from the agent, an imperfect and after-the-event remedy at best.

9.18. Sections 35 of the AML/CFT Act affirms the limited purpose for which shared information can be used, reminding agents and third party outsourced providers of a key data protection/privacy principle that information shared with them can only be used for the particular purpose engaged, being AML compliance, and no other purpose.

Data usage and controls when the Police handle private information

9.19. A different example of information sharing and usage issues concerns the ways in which the Financial Intelligence Unit uses and discloses information. The FIU requires entities to only provide SARs to it via a secure purpose-built reporting portal online, named "GoAML". The FIU then can and does routinely aggregate and use suspicious reporting information it has collected lawfully under the AML/CFT Act and Regulations.[87] Other units within the New Zealand Police end up being one of the biggest customers of the FIU, through various operational specialist teams that receive FIU analysis reports and related products – especially the Money Laundering Team investigations. The FIU also contributes to other government and law enforcement agencies more widely, such that there is regular public sector data sharing with New Zealand Customs, Inland Revenue, Immigration agencies and the Serious Fraud Office.

9.20. The FIU's Suspicious Reporting guideline states "*the FIU discloses information to the appropriate agencies for the purposes of national security, counter-terrorism, countering weapons proliferation, and transaction and serious organised crime*". [88] Inevitably, a frequent exchange of data would be needed for international law enforcement agency channels to operate effectively. Section 143 of the AML/CFT Act expressly gives the FIU power to share intelligence data with "regulators and domestic and international authorities".

9.21. Section 137 of the AML/CFT Act contains rules for the Supervisors' use of and sharing of information.

9.22. The Financial Crime Prevention Network ("FCPN") is an informal group created in the last few years for the NZ Police to work in a type of public-private partnership with large reporting entities. It was formed in order to share information about specific criminal operations or active areas of interest. The objective of this network is said to be to "prevent financial crime; protect our economy and our people; and above all else, prevent organised crime from flourishing in New Zealand and combat terrorist financing."[89]

9.23. This approach follows successful information exchange fora developed in other jurisdictions, such as the Joint Money Laundering Taskforce (JMLIT) in the UK, and the Fintel Alliance in Australia.

9.24. New Zealand's FCPN serves to enhance the response to particular criminal threats, including terrorist groups or child exploitation and other forms of trafficking crimes, by more interactive and deep

---

[87] Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Regulations 2011 (SR 2011/225) (as at 01 August 2019) Contents – New Zealand Legislation.
[88] NZ Police FIU Suspicious Reporting Guideline, 2018 at 31 suspicious-activity-reporting-guideline.pdf (police.govt.nz).
[89] New Zealand Police "Financial Crime Prevention Network" https://www.police.govt.nz/advice-services/businesses-and-organisations/nz-financial-intelligence-unit-fiu/financial-crime.

communication with a chosen group of large private sector parties. The FIU leads the FCPN, whose other members comprise of New Zealand Customs and the nations' largest 5 retail banks: Australia New Zealand Banking Group (ANZ), ASB, Bank of New Zealand (BNZ), Kiwibank and Westpac. These large reporting entities represent the ones who, by volume, provide the most SARs to the Police over time.

9.25. The FCPN Operations Board meets regularly to discuss current financial crime trends. The FIU frequently issues a request for data about a current operation a "FIU Alert") to these main banks, who can then submit tailored and deep reports in response. This forum is used to share operational priorities in order to develop intelligence that draws on the collaborative knowledge-base of all its members. This is one of very few ways in which banks may directly share information about accounts, activities or customers – inside the safe haven of a FIU focus group. In addition, joint strategic products are developed to inform guidance for both FCPN members and the broader set of Reporting Entities who are not within the FCPN club.

9.26. Banks themselves sometimes clamour to be able to share data more proactively amongst themselves. In a submission to the Parliamentary Select Committee considering the Phase 2 AML/CFT Amendment Bill in 2017, the New Zealand Bankers Association trade body argued that the AML regime would benefit greatly if reporting entities were able to share financial intelligence/customer information with other reporting entities (although only in tightly defined circumstances).[90] Further, banks claimed this would enhance the ability of reporting entities to rule out activity that might otherwise appear suspicious - in the absence of additional information that one entity alone may not have access too. Hence this would improve the quality of their suspicious transaction reporting. They point to a similar sort of ability in the USA's Patriot Act 2001, where section 314(b) of that legislation allows US financial institutions the ability to share information with one another in order to better identify and report potential money laundering and terrorist activities. Controls in that provision require financial institutions to establish and maintain procedures to safeguard security and confidentiality, notify authorities that they are sharing information, and it must only be used for strictly limited purposes.

9.27. That sort of more widespread private sector data-sharing, without oversight of the Police FIU, has been resisted so far in New Zealand. It would engender far more serious privacy rights concerns if permitted. There have been many incidents of "false positives" and unfair closures of bank accounts even with one bank acting on its own information, so the potential for banks to act jointly upon such issues is troubling. That leads into areas where another regulator, the Privacy Commissioner, might have something to say.

Privacy law requirements and the Privacy Commissioner's role

9.28. Reporting entities under the AML/CFT Act must have regard to privacy issues and protect personal information they hold in respect of the supply, and use of information among DGBs or related companies.

9.29. The Privacy Act 2020 governs personal information collected and held by entities in New Zealand (or potentially about New Zealanders). The definition of personal information is very wide to cover any "information about an identifiable individual" – i.e. not a legal person/company. This Act revolves around 13 information privacy principles relating to the collection, use and disclosure of personal information, overseen by the Privacy Commissioner. The principles aim to ensure that personal information is only collected by lawful means, not held for longer than necessary, is kept secure and not disclosed except in certain circumstances, and that the person to which the information relates to has access to it, and opportunity to correct errors.[91]

---

[90] Submission to the Law and Order Select Committee on the Anti-Money Laundering and Counter Financing of Terrorism Amendment Bill by the New Zealand Bankers Association, April 2017: https://www.nzba.org.nz/wp-content/uploads/2017/04/170420-NZBA-Submission-Anti-Money-Laundering-and-Countering-Financing-of-Terrorism-Amendment-Bill.pdf.

[91] Specifically principles 3–11 in Part 2 of the Privacy Act 2020 cover storage, access to and accuracy of personal information held, and limits on its use and disclosure.

9.30. An example of how entities must try to balance the competing legal principles comes in the mundane area of record-keeping. Entities must meet specific obligations in ss 49–53 in the AML/CFT Act to keep careful records, for at least 5 years in most cases. But once those periods expire, as a concession to privacy law tensions, the entities must then under s 54 of the AML/CFT Act take steps to ensure that every record retained is destroyed as soon as practical (subject to any other legal requirements). This reminds entities they must not retain the data for longer than necessary, where it may impact on client privacy.

9.31. However, where the direct policy needs of the AML regime are more important, the AML/CFT Act over-rides the Privacy Act principles. For instance, privacy law generally requires good reasons for disclosing personal information to anyone other than the data subject person, and for use of the information for any reason other than the purpose for which it was originally collected. A legal obligation upon a bank to make a report passing information about a person's suspicious activity is clearly an express and necessary over-ride. Similarly, the restrictions in ss 46 - 47 of the AML/CFT Act to prevent the disclosure of information to the person subject to the SAR (commonly known as "no tipping off" rules) specify certain types of information that must be kept secret, and with only a few exceptions cannot be disclosed to persons to who may ordinarily, under the Privacy Act, be able to request access to information held about them.

9.32. New Zealand's privacy regulator is given an express role in the AML regime at certain points, and has been an active contributor. For instance, before issuing suspicious activity/transaction guidelines for each type of reporting entity, setting out examples and features of transactions that may give rise to suspicion of money laundering offences, the Police must first consult with the Privacy Commissioner.[92]

9.33. When the AML/CFT Amendment Bill 2017 was being developed there was some controversy around whether officials should be able to access other public agencies' databases directly. A submission from the Privacy Commissioner to Parliament agreed that allowing direct access to databases is appropriate in some exceptional circumstances (e.g. under the Intelligence Security Act 2017 that allows intelligence and security agencies to access information by other agencies directly, given the important national security nature of their work). However, the submission urged caution, a tightening of definitions, and more safeguards around expanded public sector information sharing regulations.[93] Again, any such regulations made can only be approved by government following consultation with the Privacy Commissioner.

9.34. Some information such as access to central government data registries (e.g. land ownership, information about births, death and marriages) could be seen as less sensitive for sharing. Indeed, arrangements already in place allow both public and private sector agencies to check whether identity information presented by customers is the same as that recorded by the Department of Internal Affairs through its citizenship, passports, and Births, Deaths & Marriages registry functions. The relevant legislation and approval processes set out strict privacy controls on the circumstances in which non-published registries can be accessed.

9.35. Separately, some IT service providers and vendors of KYC software apps are compiling their own private databases that can be subscribed to by customer for a fee, in order to assist reporting entities with verification information about New Zealand citizens and residents. Apart from the broad information privacy principles in the Privacy Act, there is not yet any specific regulation of these emerging electronic verification and digital identity markets.

9.36. The same issue came up in a separate but related legal topic, the international transfer of tax information (under auspices originally of the US FATCA and then more generally the CRS or common reporting standards between nations). The Privacy Commissioner made a submission to the Parliamentary

[92] See ss 145-146 of the AML/CFT Act.

[93] Submission on the Anti-Money Laundering and Countering Financial of Terrorism Amendment Bill, as at April 2017 FINAL-Privacy-Commissioners-submission-on-AMLCFT-Bill-A498333.pdf.

Committee examining the relevant proposed Taxation Amendment Bill,[94] and agreed that proposals to implement forced disclosure requirements for foreign trusts can meet their policy objectives, as well as not unduly impacting on the privacy of the individuals concerned. Further the Commissioner submitted, "*the personal information implicated by the amendments is relatively restricted and non-intrusive, but it is sufficient to enable regulators to make further enquiries if required.*"

9.37. In a later part of the submission the Privacy Commissioner agreed that reporting entities should be allowed to share suspicious transaction related information with their parent companies, and other internal tax or financial crime monitoring teams. This enhances ability to leverage knowledge and expertise from other subject matter experts within the organisation, to assist in decision-making and the filing of reports. But that should all be kept internal, within the connected bodies of a corporate group.

Concluding thoughts

9.38. These examples show that there are a number of competing policy interests always in play. On the one hand, reporting entities, DBGs and outsourcing provider companies need access to various data-streams to be able to do their job properly. But there is the potential for this information to reveal private and deeply sensitive information about a person – pitting Privacy laws and AML/CFT Act against each other. A balancing act is at work, at a policy level within the AML/CFT Act, and at a micro-level for each reporting entity trying to achieve balance in these competing obligations. In blunt terms, entities need to effectively discharge their "unpaid financial detective" job properly, gathering and monitoring information as required by law, but also act in the public's interest and have controls that respect a person's privacy rights in the information being collected. The restrictions built into the statutes, plus the consultation with the Privacy Commissioner, helps strike the right balance to safeguard a person's private information.

9.39. However, this area is changing fast. An enormous set of issues looming for the AML/CFT regime in future will be how the coming developments of artificial intelligence, deep faking of ID, and digital identity rights which place some level of data sovereignty back with the consumer, are all balanced with the ever-increasing demands of law enforcement agencies for more and better data from regulated entities.

9.40. There is an important statutory review process taking place later in 2021, with New Zealand's AML/CFT Act over a decade in operation now, and with our latest global evaluation report by the FATF about to be released for public scrutiny. It is to be hoped that privacy and information-sharing problems will receive a thorough consideration in this process. Additionally, from years of experience, I would suggest there are a few other significant areas for improvement which, at a high level, New Zealand has to date not got right.

9.41. Overall, in my opinion, our AML/CFT system has been a beneficial step, and vastly improved our ability to dismantle crimes of profit, from where New Zealand was in 2009. Together with the very active asset recovery work that the Police carry out, it must be considered a success. However, for the business community, that has come with considerable cost, probably larger compliance costs than were needed (although the government has never performed a thorough expert cost-benefit analysis) – and those are often passed on to the consumer. Therefore, in reforming a complex system like this, close attention needs to be given to:

- Reducing complexity, duplication, and compliance costs, which can damage a willingness to comply;
- Greater consistency of regulatory outcomes, including which various agencies and how many should be involved;
- Better mechanisms into handling risks around beneficial ownership and opaque structures.

[94] Submissions to the Finance and Expenditure Committee on the Taxation (Business Tax. Exchange of Information, and Remedial Matters) Bill 149-1 2016-Sep-Privacy-Commissioners-submission-to-Finance-and-Expenditure-Committee-on-Tax-Bill-149-1.pdf.