NEW ZEALAND'S NEW AML/CFT REGIME
A brief overview and some challenges – will it stand the test of time?

Paper prepared for the Banking & Financial Services Law Association
2013 Annual Conference

Bradley Kidd, Partner, Chapman Tripp

The New Zealand Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the *AML/CFT Act*) has been, in terms of systems impact, one of the largest changes for banks and financial institutions in the last ten years.

This paper outlines key elements of the new regime, the challenges that exist, and concludes with a discussion of implementation issues that remain with the legislation.

KEY ELEMENTS

The AML/CFT Act came into force on 30 June 2013 for banks, casinos and other financial institutions. Certain other types of professionals and businesses (including lawyers) will be required to comply with the legislation at a point in the near future.

The Ministry of Justice has overseen the development and implementation of the regime. Unlike most other countries, New Zealand has chosen to adopt a split supervisory model with the Reserve Bank, Financial Markets Authority and Department of Internal Affairs acting as the lead supervisor of their relevant sectors.

The AML/CFT Act broadly requires reporting entities to conduct customer due diligence and to monitor their accounts and transaction behaviour. These two major components can be broken down further into several discrete obligations.

The key conceptual underpinning of the AML/CFT Act is that entities subject to it can take a "risk-based" approach to compliance. While that is attractive in theory – entities can calibrate their compliance according to the level of money laundering or terrorism financing risk – it comes at the price of certainty as to what the precise obligations require.

A. Application to reporting entities

The AML/CFT Act applies to reporting entities, defined to be either financial institutions, casinos, any person or class declared by regulations to be a reporting entity under the Act, or any other person required to comply under any other enactment.

Financial institutions are further defined as those who, in the ordinary course of business, carry on one or more of fifteen listed financial activities that, among others, include:

- accepting deposits from the public;
- lending to or from customers;
- trading in various financial instruments; and
- participating in securities issues and financial services relating to those issues.

Banks and financial institutions are the core of the regulated sector due to the number of activities they perform and the volume of transactions they process.

The remaining entities that are subject to the regime - now and in the future - form a disparate group whose common feature is that the business they conduct or the services they offer are considered to be vulnerable to money laundering or terrorist financing.

Interestingly, and somewhat frustratingly for lawyers and industry alike, the categories of "financial institution" do not match the equivalent definition in the Financial Service Providers (Registration and Dispute Resolution) Act 2008, which was a precursor to the AML/CFT Act (and established a register of financial service providers as a first stage to the anti-money laundering reforms in New Zealand).

B. Key preliminary matters

Prior to 30 June 2013 reporting entities were required under the AML/CFT Act to:

- undertake a risk assessment of their business;
- prepare a compliance plan; and
- appoint a compliance officer.

The first two items have been significant exercises for many financial institutions, and have also necessitated the establishment of new and extensive compliance procedures applying across the entire customer base.

C. Targets of customer due diligence

The AML/CFT Act requires reporting entities to focus on three targets for customer due diligence: customers, their beneficial owners, and anyone authorised to act on their behalf.

- *Customer* is defined as any new or existing customer and includes any "facility holder" (which is itself defined further in the AML/CFT Act).
- *Beneficial owners* are defined as the individual(s) who have effective control of a customer or person on whose behalf a transaction is conducted, or who own 25% of the customer or person on whose behalf a transaction is conducted.
- *Persons authorised to act on the customer's behalf* refers to those persons who are authorised to carry out transactions or other activities on behalf of the customer.

Reporting entities must collect certain information from each of the persons listed above and, consistent with the fundamental premise to the AML/CFT Act, are entitled to adopt a risk based approach to verifying their identity by reference to *independent and reliable documentation or evidence*.

Identity Verification Code of Practice - The Identity Verification Code of Practice (*IVCP*) offers a safe harbour for reporting entities to meet their verification obligations under the Act. The IVCP is not mandatory, but offers a "safe harbour" for reporting entities who verify a person's name and date of birth from independent and reliable documentation (such as passports and drivers' licences). If reporting entities do not adopt the IVCP, to

have an alternative safe harbour they must notify their supervisor and explain why that alternative is equally effective to the IVCP.

The advantage of the IVCP is its flexibility. Unlike the comparable Australian 100 point identity verification system, the IVCP is relatively non-prescriptive and allows reporting entities to adopt a risk based approach to methods of identity verification.

The primary disadvantages of the IVCP are twofold:

- it only covers name and date of birth verification. Verifying an address – which is a requirement under the Act – must be done by reference to data or information from a reliable or independent source, but acceptable sources are not defined; and

- it only applies to customers who a reporting entity classifies as low or medium risk. Higher risk customers must be subject to "increased or more sophisticated measures" (and there is no explanation of what those measures may be).

These details appear relatively minor, but they take on a new significance when applied to banks and other major financial institutions, where the legal nirvana would clearly be a universal safe harbour.

D. Tiers of customer due diligence

The AML/CFT Act allows reporting entities to adopt a three tiered approach to customer due diligence (*CDD*): standard, simplified and enhanced CDD.

Standard CDD is the default setting under the Act, and applies:

- when a reporting entity establishes a business relationship with new customer;

- if a customer seeks to conduct an occasional transaction via the reporting entity;

- if there has been a material change in the nature or purpose of the business relationship with an existing customer or the reporting entity considers it does not have sufficient information about the customer.

Standard CDD requires the reporting entity to collect the person's full name, date of birth, address, and company registration details (if any), along with information on the nature of the reporting entity's relationship with that person.

Simplified CDD applies in narrow circumstances for low risk individuals such as listed companies, local authorities and government departments. The regulations contain additional entities that are subject to simplified CDD, including Crown entities, statutory supervisors or trustees, and trustee corporations.

Where simplified CDD applies, the reporting entity need not ascertain the person's address and is *not* required to identify the beneficial owners of the customer.

Enhanced CDD applies for customers who are deemed to present a high risk of money laundering. Amongst other situations, it applies:

- where the reporting entity establishes a business relationship with a trust, a company with nominee shareholders, or a politically exposed person (*PEP*);

- when a customer seeks to conduct a complex and unusually large transaction; or

- where the reporting entity considers that the level of risk involved is such that enhanced CDD should apply.

When enhanced CDD applies the reporting entity must, in addition to the requirements of standard CDD, *also* collect information on the source of funds or wealth of the customer.

E. Other obligations

The AML/CFT Act also requires reporting entities to meet a series of obligations that broadly fall into the customer due diligence categories, including:

- identifying and verifying the identity of PEPs;

- tracking and tracing the proceeds of domestic and international wire transfers (the most onerous obligations unsurprisingly apply to international wire transfers); and

- identifying the beneficiaries or class of beneficiaries of trusts.

Identifying whether a customer is a PEP is a particularly onerous obligation. PEPs are individuals who have held prominent positions of authority in any overseas country within the preceding 12 month period (and their immediate family members). Section 26 requires reporting entities to take reasonable steps to determine whether a customer or beneficial owner is a PEP at the time they establish a business relationship or conduct an occasional transaction. Once a PEP is identified, they are then subject to enhanced CDD. Compliance with this obligation is especially difficult for small to medium sized financial institutions, which may not be able to afford sophisticated systems to automate the PEP screening process. Even reporting entities with sufficient scale will find it challenging to implement automated systems that are capable of screening new customers against extensive databases merely to isolate the few individuals who meet the definition.

Wire transfers contain an entirely separate set of obligations under the AML/CFT Act that require reporting entities to capture information on both the originator and the beneficiary of certain wire transfers that exceed cash value limits specified in the regulations. These requirements are of particular relevance to banks and international money remitters.

Trusts are subject to enhanced CDD and, in addition, the regulations *also* impose an additional obligation on reporting entities to obtain the name and date of birth of each beneficiary, or the class of any discretionary beneficiaries of every trust they deal with. This obligation can be burdensome for reporting entities, particularly in New Zealand, where historic preferential tax treatment led to a proliferation of family trusts as vehicles for holding relationship property.

F. Record keeping

Record keeping is required by reporting entities after they have collected and verified this information. In particular:

- *Section 50* requires a reporting entity to retain the verification records for at least five years after the business relationship ends or the occasional transaction is completed.

- *Section 49* requires that for every transaction, sufficient records must be kept to allow the transaction to be readily reconstructed. At a minimum this requires the reporting entity to retain a record of the nature, value, currency, date, parties and accounts for at least five years after the transaction is completed.

G. Ongoing customer due diligence and account monitoring

The second major component of the AML/CFT Act (contained in section 31) shifts the regime from a static collection to a dynamic monitoring regime by requiring reporting entities to conduct on-going customer due diligence and account monitoring.

Ongoing customer due diligence is not well defined in the legislation or explained by later guidance. The AML/CFT Act simply states that reporting entities are required to "regularly review" the information collected from their customer due diligence processes. This leaves reporting entities with a relatively blank canvas on which to design a solution that complies with this obligation. It is very difficult to ascertain what the supervisor's expectations are for reporting entities who wish to comply with this obligation. Clarity would be welcome.

Account monitoring is ultimately a major compliance component of the legislation. It requires reporting entities to adopt systems and processes that enable them to regularly review their customers' accounts and transaction behaviour in order to identify suspicious activity. Once this activity is discovered the AML/CFT Act places a positive obligation on the reporting entity to file a suspicious transaction report.

Suspicious transaction reports contain all of the information that the reporting entity has collected on its customers' identity via its CDD procedures, along with the account and transaction activity monitored under section 31 and retained under sections 49 and 50. These reports are typically uploaded electronically directly to the Financial Intelligence Unit of the New Zealand Police through its "goAML" platform. The information may ultimately go on to provide a basis for an investigation and potentially a prosecution.

H. Other ongoing requirements

Other key ongoing compliance obligations on reporting entities include:

- a two-yearly audit of the risk assessment and compliance programme

- an annual report to the relevant supervisor (the content of which is heavily prescribed, and necessitates the collection and presentation of a wide variety of information).

CHALLENGES

A. Fragmentation of obligations and supervision

Fragmentation of obligations and information remain a key challenge for reporting entities seeking to comply with their AML/CFT obligations.

The obligations under the AML/CFT regime essentially come from four separate sources:

- the AML/CFT Act
- three sets of Regulations
- codes of practice; and
- guidance notes and fact sheets periodically released by the supervisors.

Reporting entities are required to comply with what they could be forgiven for seeing as a bewildering array of obligations and guidance. There is a risk that this regulatory complexity may in turn lead to inconsistencies in implementation across the financial sector.

The joint supervision model with the Reserve Bank, Financial Markets Authority and Department of Internal Affairs acting as supervisors for their respective areas has advantages and disadvantages:

- *Advantages*: the model provides a better fit for reporting entities to be supervised by agencies who better understand the business and structure of each sector. Another advantage is regulatory expertise and the sharing of ideas.
- *Disadvantages*: assistance (whether by guidance note or otherwise) can take more time depending on the resources available to each agency due to the need for co-ordination between supervisors. There is also the potential for divergent approaches between the supervisors; but this risk has not been observed in practice as a result of the careful co-ordination between the supervisors.

B. Difficulties in determining the Act's application

The AML/CFT Act can apply over-inclusively to entities who would not consider themselves to be a financial institution, but who must nevertheless comply because a small or ancillary part of their business involves one of fifteen listed activities in the Act's definition. The lack of alignment with the Financial Service Providers (Registration and Dispute Resolution) Act 2008 is a significant contributor to this issue.

This uncertainty arises because a financial institution is defined not by reference to a class of entities, but by reference to the types of financial activities those institutions typically perform. Where entities conduct these activities as only an ancillary part of their business, imposing an obligation to ensure they have sufficient systems and processes to comply may increase transaction costs and impose a significant regulatory burden.

There are few safe harbours offered by the AML/CFT Act, and further policy work in this area would be welcome, especially for medium sized financial institutions who must carry the full burden of the regime but who may lack sufficient resources and scale to develop a fully compliant solution.

C. Third party reliance

Reporting entities will often need to rely on third parties to meet some of their CDD obligations under the legislation. They can do so in two ways:

- *Section 33* provides a means by which a reporting entity may rely on another reporting entity or overseas person to conduct CDD. This is permitted in very narrow circumstances and the requirements are highly prescriptive.

- *Section 34* allows a reporting entity to authorise a person to be its agent and rely on that agent to conduct CDD and obtain any other information required to comply with the AML/CFT Act or its regulations.

Aside from the designated business group regime (which while delivering some significant gains, is far from perfect), there are no other mechanisms by which reporting entities can rely on third parties to conduct CDD on their behalf. Even where they do rely on agents or third parties to do so, they ultimately remain responsible for insuring that the third party complies and will remain liable if they fail to do so.

To date only very limited guidance has been forthcoming from the supervisors on how issues of intermediation and third party reliance are to be implemented.

Reporting entities may also face difficulties in situations where they might wish to rely on third parties to conduct CDD on their behalf, but the transaction costs and compliance risks associated with appointing an agent via contractual arrangements are prohibitively high to allow this to occur. A middle way may be required.

D. Beneficial ownership

Ascertaining who the beneficial owners of a customer are (i.e. individuals with effective control or a holding of more than 25% of a customer) will continue to be a particularly complex area of the legislation. The supervisors have provided some clarity in relation to this obligation through the publication of a general guidance note on beneficial ownership, along with a recently issued draft fact sheet on managing intermediaries.

The draft fact sheet relates specifically to the apparent 'third limb' of the definition of beneficial ownership, being the requirement to identify the "individual who has effective control of a … person on whose behalf a transaction is conducted".

The interpretation of this limb of the definition has created uncertainty in the managed funds industry, especially for reporting entities (such as banks) who provide financial services to managing intermediaries – entities who manage funds on behalf of others, such as fund managers, financial advisors and trustees/custodians. Consultation on the draft fact sheet is still underway, and industry will no doubt watch with interest for the outcome.

IMPLEMENTATION AND NEW TECHNOLOGIES

New technologies and greater interconnectivity with customers are pushing the boundaries of a regime that is largely set against a traditional, paper based, face-to-face paradigm. Technology is rapidly expanding the ways in which customers are able to interact with financial institutions.

There are more products, more services, and more platforms today than when the AML/CFT Act was introduced, and more will be developed in the future. Today customers expect to conduct their banking through smartphones and internet platforms, not branches and call centres. They increasingly utilise new payment methods that offer a degree of

anonymity, such as stored value instruments, prepaid cards, micro lending and digital currencies.

All of these new technologies rely, at least in part, on customers being able to interact with a financial institution immediately in real time. Anti-money laundering controls must be able to keep pace with this change in usage. Customers will increasingly come to expect that they will be able to set up facilities over the internet, through their tablet or on a smartphone.

This will in turn require banks and other financial institutions to develop innovative and new methods of complying with their AML/CFT obligations through conducting risk assessments and electronic identity verification in real time. We are starting to see the development of new solutions to meet these demands. The introduction of services such as RealMe, an online electronic 'passport' that can integrate with banks electronic identity verification systems, is one such example.

The question to conclude with is whether these new technologies will in turn create an AML digital divide between those financial institutions who can afford to build compliant AML solutions and those who cannot? In the end a balance must be struck between allowing for financial innovation and controlling the money laundering risks presented by these new products and services. The right place to strike this balance must always inform regulatory development in this area, and we must remain optimistic that it will drive the continuous improvement of New Zealand's AML/CFT regime.

Acknowledgement

My thanks to Brendon Orr, Solicitor, Chapman Tripp for his assistance with this paper.