Your guide to the Anti-Money Laundering and Countering Financing of Terrorism Act

This eBook introduces and discusses some of the obligations imposed on reporting entities.

bartercard

Contents

Introduction

On 30 June 2013, the Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) Act 2009 came into effect in New Zealand. The Act imposed a number of obligations on banks, fund managers, financial advisers, debt collectors, safe deposit box vaults and numerous other entities, and was designed to ensure such businesses and financial institutions were able to detect and report potentially criminal origins or purposes of money.

The introduction of this legislation had an immediate effect on consumers; new requirements for establishing new and continuing existing business relationships, along with those entities covered by the act now having to monitor and report all suspicious transactions.

These legislative requirements are now being extended to the legal, real estate, sports betting and high value goods industries (jewellery, precious metals, precious stones, watches, motor vehicles, boats, art or antiques where they take cash payments of $15,000 or more), and will come into effect from mid-2018 to mid-2019. It is likely that it will more than quadruple the number of businesses in New Zealand required to contend with AML requirements.

Did you know?

High value goods businesses will need to comply with the AML/CFT Act if they accept cash payments of $15,000 or more, regardless of whether it is in one payment or a series of installments that total $15,000 or more. If those businesses do not accept cash transactions of that size, they do not have to comply with the legislation.

With the legislation now being in force for several years and a shift from warning to prosecution by AML Supervisors, it is important that businesses take their obligations seriously and understand the role they play in ensuring AML processes and structures are in place ahead of the legislation coming into force for their industry.

This eBook introduces and discusses some of the obligations imposed on reporting entities.

What every business needs to do

Under the legislation, each reporting entity needs:

- A Risk Assessment of the potential for your business to be exposed to money laundering and financing of terrorism activities
- An AML/CFT Programme with procedures to detect, deter, manage and mitigate the possibility of money laundering taking place
- A Compliance Officer appointed to administer and maintain your AML/CFT programme
- Customer Due Diligence processes including customer identification and identity verification
- Suspicious Transaction Reporting, Auditing and Annual Reporting processes
- To file an annual report with their supervisor (the Reserve Bank of New Zealand, the Financial Markets Authority or the Department of Internal Affairs).

Risk Assessment

The first step a business must take is to identify and assess the risks that they face in the normal course of their operation relating to money laundering or the financing of terrorism. This assessment must be in a written form and it has to set out how this assessment will be kept up-to-date. Once this has been written, it is then used to develop the AML/CFT Programme for the business.

Among the factors that have to be taken into consideration in assessing the risk are:

- The nature, size and complexity of the business
- The products and services the business offers
- The way the business delivers its products and services
- The types of customers the business deals with
- The countries the business deals with, and
- The institutions the business deals with.

Risk assessments must be independently audited every two years. The annual report that must be filed with a businesses' AML supervisor includes information on this aspect.

AML/CFT Programme

The AML/CFT Programme sets out the internal policies (the standards and behaviours of the business), procedures (the detailed day-to-day means of operations) and controls (the tools used to ensure the business complies with the policies and procedures) to detect attempts to launder money or finance terrorism.

The programme must cover:

- **Vetting –** checking the background of senior managers, the compliance officer and any other employees who have AML/CFT duties, to determine their suitability for that position
- **Training –** to ensure the relevant employees are aware of the risks faced by the business and how they should respond to such risks
- **Written findings –** how the business will monitor, examine and keep written reports on any activity that by its nature is likely to be related to money laundering or the financing of terrorism, any complex and/or large transactions with no obvious economic or lawful purpose or any business relationships or transactions with countries that are AML/CFT risks
- **Record Keeping –** records need to be kept for a minimum of five years after a transaction or after the business relationship has ended
- **Products and transactions that favour anonymity –** any products that the business offers that might favour anonymity have to be identified and detailed as to how the business will prevent their use for money laundering or financing terrorism
- **Managing & mitigating risk –** how the business will ensure that it remains up-to-date with combatting new risks of money laundering or financing terrorism

- **Ensuring compliance with the AML/CFT programme –** how the business will monitor their AML/CFT programme to make sure that it is effective and meeting the business' obligations under the legislation
- **Review and audit of the AML/CFT programme –** the programme must be independently audited every two years (or whenever the supervisor requests it) along with being regularly reviewed by the business
- The **Customer Due Diligence process** for the business
- **Suspicious transaction** and **activity reporting.**

Compliance Officer

One of the most important aspects of the AML/CFT system for any reporting entity is the Compliance Officer. An employee must be designated to administer and maintain a business' AML/CFT programme. This does not have to be a standalone position, so the role can be carried out by an existing employee in addition to their existing duties, but their job description must be updated to reflect the Compliance Officer role. The role must report to a senior manager of the reporting entity with access to any board of directors or relevant management committee.

Most importantly for the Compliance Officer themselves, they are personally liable for breaches of the Act, the penalties for which can be up to $200,000 per breach. As such, they have a substantial stake in the business meeting legislative requirements.

Customer Due Diligence

A major component of the AML/CFT system is Customer Due Diligence which must be performed on new customers. While the same requirements do not immediately apply to existing business relationships, there is the expectation that when there is a material change to that business relationship, the client will be subject to Customer Due Diligence.

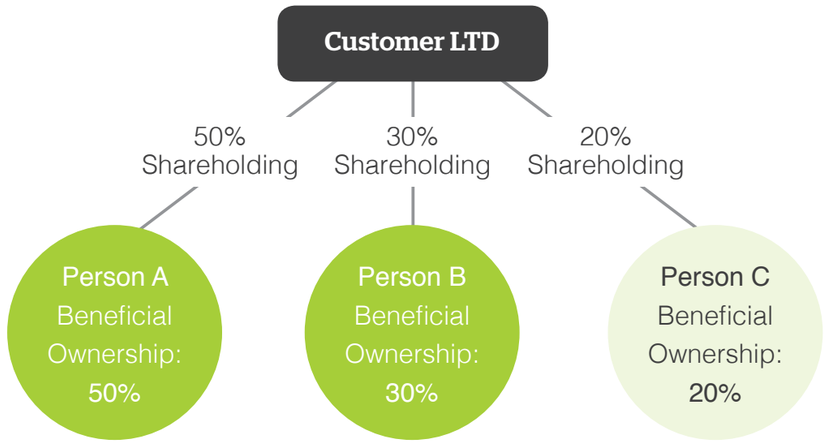
It is also expected that it will be necessary to carry out Customer Due Diligence on all existing business relationships in the future. It is therefore advisable for any reporting entity to establish a process for performing Customer Due Diligence on their existing customer relationships.

Under the Act, reporting entities are required to undertake Customer Due Diligence on:

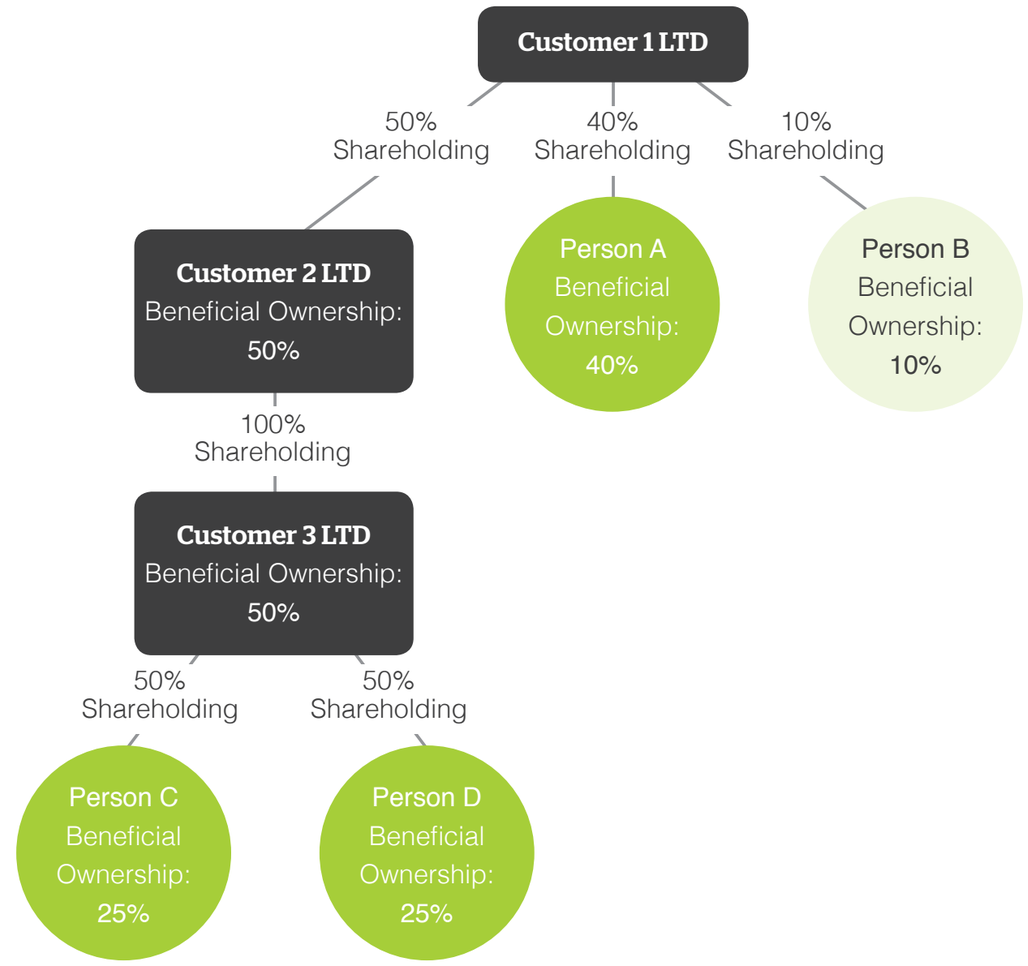
- A customer
- Any beneficial owner (an individual who owns 25% or more of the customer or has effective control of that customer)
- Any person acting on behalf of a customer.

Any information collected in the Customer Due Diligence process is still covered by privacy legislation in the same way as any other information collected about customers.

Establishing who the beneficial owners of a customer are so they can be identified under Customer Due Diligence can sometimes be tricky. When dealing with companies, it involves going through the shareholding to figure out who reaches the 25% ownership threshold. For example in the following scenario:



For a company establishing a business relationship with *Customer Ltd*, they will need to identify *Person A* and *Person B* as they hold 25% or more of the shareholding in the company. There is not a need to identify *Person C* as they do not reach that threshold. If *Person C* is acting on behalf of the company in the relationship with *Customer Ltd*, then they will still need to be identified. In the following scenario:



A reporting entity seeking to establish a business relationship with *Company 1 Ltd* would need to conduct Customer Due Diligence on *Person A, Person C* and *Person D*. *Person A* has 40% ownership of *Company 1 Ltd* so is clearly required to be identified. Because 50% of the shares of *Company 1 Ltd* is owned by *Company 2 Ltd* which in turn is 100% owned by *Company 3 Ltd*, the two shareholders of *Company 3 Ltd* effectively control 25% of *Company 1 Ltd* each.

Suspicious Activity & Transaction Reporting

While much of the administrative effort around AML/CFT is based on identifying customers, monitoring transactions and reporting suspicious transactions to the Police Financial Intelligence Unit is just as important an aspect of the legislation.

The Police run training sessions for their goAML web reporting portal so businesses know how to go about reporting suspicious transactions through the online system.

The most important aspect, however, is understanding when a transaction or a customer's activity is suspicious. This comes down to knowing your customer so you are able to tell when their activity is unusual or out of step with what you would normally expect for that type of customer.

International wire transfers of $1,000 or more and any physical cash transaction of $10,000 or more must be reported to the Police Financial Intelligence Unit. For high value goods dealers, they will have to file reports on any cash transaction of $15,000 or greater, and may file a report on suspicious activity that does not result in a transaction.

Some "red flags" for potentially suspicious activity include:

- Overpayment of amounts with a request for refund of the balance
- A customer requests that funds that are overpaid or no longer required are refunded to a third party rather than back to themselves
- Amounts being deposited are large compared to the customer's income
- Regular buying and selling of valuable items or commodities that don't make economic sense
- Complex ownership structures.

Conclusion

AML adds a significant amount of administration and information gathering for businesses in order to comply with the law. The penalties are significant and with Phase 2, the amount of businesses that have to comply will increase substantially. While this will mean that customers will become more used to having to provide the information required in their interactions with a number of different industries, it is still the responsibility of affected businesses to ensure that they comply with the law.

bartercard

HAVE A QUESTION ABOUT WHAT BARTERCARD IS OR ISN'T?
Visit askbartercard.co.nz

For more information about Bartercard please visit our website, or follow us on LinkedIn, Facebook and Twitter.