# NZ AML SUMMIT 2015

## AML Solutions Answers Your Questions

1) Can you rely on public information for charitable and Maori trusts e.g. Land settlements?

   Where that information is sourced from independent and verifiable sources, such as Government websites, you may seek to rely on this information. You will still need to ensure that those websites contain the information required under the '*Customer Due Diligence – Trusts*' Fact Sheet in respect of the trust and beneficiaries and of course identify and verify any relevant natural persons.

2) Please clarify trust verification. I thought we needed only names and DOBs for beneficiaries.

   Regulation 6 of the Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Regulations 2011 provides additional information on enhanced CDD for the beneficiaries of trusts. Regulation 6(1) requires you to obtain the name and date of birth of each beneficiary of a trust. However, regulation 6(2) allows you to relax this requirement if your customer is a discretionary trust, a charitable trust, or any type of trust that has more than ten beneficiaries. In such cases you must obtain:

   a. a description of each class or type of beneficiary, and

   b. in the case of a charitable trust, the objects of the trust.

   In addition to collecting the above information, beneficiaries of a trust that have a vested interest[1] of at least 25% in the trust property will be 'beneficial owners'[2]. Where a beneficiary of a trust is a beneficial owner, then full CDD will have to be completed on such person in line with the Amended Identity Verification Code of Practice 2013.

3) Can we have some comment on the AML and CDD challenges when clients die and ownership of their account reverts to their estate?

   In the application of CDD to a deceased estate, we take guidance from the approach to trusts (as an estate is a form of testamentary trust) and therefore apply the requirements applicable to a trust under the Act and associated guidance including the '*Customer Due Diligence – Trusts*' Fact Sheet, albeit with some minor amendments to address practical requirements.

   For example, the Fact Sheet contemplates that the settlor of a trust will be identified and verified in line with the Act. In the case of estates, an entity may consider relaxing this requirement, instead relying on the death certificate or grant of probate to evidence the deceased's identity. This also allows for the practical difficulty of obtaining identification of the deceased in line with the Identity Verification Code of Practice 2013 as:

---

[1] A vested interest: this is where the trust fund vests in the beneficiaries on the date the trust winds up. The beneficiary's interest is guaranteed to be received as the trust fund automatically vests in the beneficiaries named in the trust deed on winding up.

[2] See letter from the AML/CFT Supervisors dated June 2013 entitled '*Clarification of the position the AML/CFT supervisors are taking with respect of the AML/CFT Act interpretation of a trust as a customer*'.

a. The reporting entity will not be able to meet the customer face-to-face to collect original documents; and

b. it will be difficult for a trusted referee to correctly certify documents, particularly in respect of certifying a true likeness.

You will also need to have a specific consideration of whether any of the beneficiaries need to be identified and verified if the estate has vested – see 2) above.

4) Regarding electronic identity verification (**EIV**), what would you recommend as a good system for a smaller organisation?

Some EIV providers provide a scalable product for smaller entities where the EIV system need not be integrated into the entities system but, for example, can be utilised through a web browser. We would recommend contacting these providers for options.

5) As an AML auditor, what unique challenges have you seen when auditing EIV-dominated programmes?

Entities who intend on using EIV should ensure that they look at the requirements in the Amended Identity Verification Code of Practice 2013 and ensure that they cover off why they consider their approach to EIV to be effective in their AML/CFT Compliance Programmes.

Even if you are using EIV, you should ensure you have an option to utilise documentary verification if EIV is unsuccessful. Your policies and procedures should be clear as to how this will work in practice.

6) Do you apply a materiality threshold for suspicious transactions?

Strictly speaking, there is no materiality threshold in the legislation or associated guidance. If the reporting entity determines it to be suspicious, then it must report it regardless of the size or value of the (proposed) transaction.

That said, an organisation may look to apply a level of materiality in the detection of suspicious transactions. For example, an entity may adjust monitoring rules to exclude transactions below a certain value so as to better focus its investigation on those alerts which are likely to have a higher impact. This matter will depend on the organisation; what might be a small transaction for one entity may be large for another. The entity's Risk Assessment should support this approach.

7) The traditional view of money laundering is focussed on cash transactions. To what extent is this shifting to utilising electronic funds transfers and existing NZ banking systems?

Cash is still widely used in money laundering. Data from overseas suggests that cash smuggling is still one of the main methods of moving funds across borders. That said, where certain methods of money laundering are cracked down on, other methods will rise in popularity. We have seen this in the rise of trade-based money laundering, for example.

In our experience, entities tend to have better existing knowledge of the risks around cash in part because of the focus on cash under the Financial Transactions Reporting Act 1996. As more time is

spent looking at other risk areas, however, we expect those risks, from electronic transfers for example, will be better understood.

8) Do facilities such as RealMe provide any opportunities for centralised CDD of individuals in NZ?

RealMe is certainly intended to act as a centralised store of individual CDD information. One challenge for the product is that it requires an individual to present themselves at a Post Office with their identity documents to become verified. It does not allow reporting entities to share CDD information that they currently hold with each other – i.e. a "CDD bureau".

The benefit of a CDD bureau (as discussed by Roger Wilkins) is that it would allow entities to use the wealth of existing information that they hold, rather than force the customer to be identified and verified again. However as discussed at the conference, this may require revisiting some of the current privacy legislation to facilitate.

9) Is there any policy or guidelines around the need to re-ID/CDD existing clients periodically?

The AML/CFT Act contemplates re-identification of existing customers on an event-driven (i.e. due to a material change in the nature and purpose of a business relationship under s14(c)) or ongoing, periodic basis (under s31). Reporting entities should ensure their Compliance Programme addresses both of these scenarios.

In terms of guidance on periodic review and updating of CDD information, there is no written guidance issued by the Supervisors to date although it is possible that there will be in the future. A common approach we have seen is to review and update every say year for a high risk customer, 2 years for medium risk and 3 years for low risk. Entities should consider their own risk assessment in setting their own review timetable.

The entities we have seen best apply this is where they take the opportunity to update CDD where they have a reason to see the customer in person - e.g. financial advisers who see their customers at least once a year or a new loan to an existing customer where the person applies in person.