What you need to know about identity verification under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (“AML/CFT Act”)

This Code of Practice has been approved by the Ministers of Finance, Commerce and Internal Affairs under section 64 of the AML/CFT Act and comes into force on 30 June 2013.

The obligation

Under section 11 of the AML/CFT Act:

“A reporting entity must conduct customer due diligence on –
   a) a customer
   b) any beneficial owner of a customer
   c) any person acting on behalf of a customer”

What does it mean?

Reporting entities under the AML/CFT Act must:

1. Obtain a range of information from customers depending on the level of due diligence required under the AML/CFT Act; and then
2. Verify that information by confirming some of that information against documents, data or information obtained from a reliable and independent source as prescribed under the AML/CFT Act.

This can be done by:

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face-to-face document verification</td>
<td>Non face-to-face document certification</td>
<td>Electronic document verification</td>
</tr>
</tbody>
</table>

The Code of Practice (“The Code”)

Do I have to comply?

• Codes of Practice are suggested best practice to assist reporting entities to comply with certain AML/CFT Act obligations.
• Complying with it is NOT mandatory and can be opted out of. However, if fully complied with, they operate as a ‘safe harbour’.
• In case a reporting entity chooses to opt out, they will not receive the benefit of the safe harbour and will have to comply with the relevant statutory obligation by some other equally effective means. A notification of opting out will need to be provided to the relevant supervisor in order to have a defence to any act or omission by the reporting entity.
• The supervisors (the FMA, RBNZ and DIA as appropriate) will consider reporting entities who comply with this code of practice to have met their obligations under section 16 (standard due diligence), 20 (simplified due diligence), 24 (enhanced due diligence) and 28 (wire transfers) of the AML/CFT Act (conditions below apply).

The conditions

The Code of Practice:

• Applies to all reporting entities in all AML/CFT sectors.
• Relates only to natural persons.
• Prescribes best practice only when conducting name and date of birth identity verification on customers (note – The Code excludes address verification for documentary verification however includes address verification for electronic verification).
• Applies only to customers that have been assessed to be low to medium risk (note - excludes high risk customers).
• Requires reporting entities to confirm the customer’s details against their own records to ensure that they are dealing with the same natural person.
The details

Option 1: Face-to-face documentary identity verification

Primary photographic ID (i.e. NZ passport)

OR

Primary non-photographic ID (i.e. Birth certificate)

Secondary photographic ID (i.e. Drivers licence)

OR

Secondary form of photographic ID (i.e. 18+ card)

Confirmation that this information presented is consistent with the information recorded by the DIA

OR

NZ drivers licence

Supporting form of ID (i.e. confirmation that the information is consistent with government registers, bank statements)

Note: When documents are not in English and it is not understood by the person carrying out the verification – an English translation MUST be provided.

Option 2: Non-face-to-face document certification

This only applies where non-face-to-face documentary verification is used and copies of identification documents are produced by the customer.

All copies of identification documents must be certified by a trusted referee of 16 years of age at a minimum.

The Code prescribes a list of trusted referees that may be used.

A certification stamp should include the following details:

I, ___________ (name), of ___________ (address), ___________ (occupation), hereby certify that I have sighted the original of this document and that this is a true copy of the original.

Signed: ___________ Dated: ___________

Note: The trusted referee MUST NOT be related to the customer.

Option 3: Electronic identity verification

Please note in your AML/CFT programme you will have to describe:

• The form of electronic verification you chose to use

• Any additional methods used to supplement your verification method

Verification from “reliable and independent” electronic sources

Name verification

At least 2 sources

Date of birth verification

At least 1 source

Address verification

At least 1 source

“Reliable and independent” things to consider

• Accurate (up to date and error rates at a minimum)?

• Secure?

• In line with Privacy Act?

• Method used to collect the information?

• Customer can be linked to the identity?

• Information maintained by a government body?

• Has it been verified by an reliable and independent source already?

While this “safe harbour” provides an opportunity to ensure compliance with the AML/CFT Act, it is not without its challenges. This Code of Practice has the potential to be complex to implement, expensive to execute and confusing for both customers and businesses alike.

To find out more on how we can assist you on your AML/CFT journey, please contact us.

Auckland

Michal Amzallag
Senior Manager, Forensic Services
T: +64 9 363 3218
E: mamzallag@kpmg.co.nz

Wellington

Troy Nicholson
Senior Manager, Forensic Services
T: +64 4 816 4839
E: troynicholson@kpmg.co.nz