AML / CFT

Anti-money laundering and countering financing of terrorism

Identity Verification Code of Practice 2011

FINANCIAL MARKETS AUTHORITY

TE MANA TATAI HOKOHOKO ~ NEW ZEALAND

RESERVE BANK OF NEW ZEALAND

INTERNAL AFFAIRS

Te Tari Taiwhenua

Identity Verification Code of Practice 2011
(Anti-Money Laundering and Countering Financing of Terrorism Act 2009 sections 16, 20, 24 and 28 for all reporting entities)

The Identity Verification Code of Practice was approved by notice in the New Zealand Gazette on the 1st day of September 2011 by the Ministers of Finance, Commerce and Internal Affairs under section 64 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act). This code of practice comes into force on 30 June 2013.

Explanatory Note:

About codes of practice
Codes of practice are intended to provide a statement of practice to assist reporting entities to comply with certain AML/CFT Act obligations. Codes of practice are dealt with in subpart 5 of the AML/CFT Act. Codes of practice set out the suggested best practice for meeting obligations. Some codes will cover all sectors, while others will be applicable to specific sectors or sub-sectors.

Complying with a code of practice is not mandatory. The AML/CFT regime allows for flexibility and scope for innovation because reporting entities can opt out of a code of practice. However, if fully complied with, codes of practice operate as a 'safe harbour'. The legal effect of a code of practice is described in section 67 of the AML/CFT Act.

If a reporting entity opts out of the code of practice it does not receive the benefit of the safe harbour. In these circumstances, the reporting entity must comply with the relevant statutory obligation by some other equally effective means. In order for this to be a defence to any act or omission by the reporting entity, the reporting entity must have provided written notification to its AML/CFT supervisor that it has opted out of compliance with the code and intends to satisfy its obligations by some other equally effective means.

What is this code of practice for?
This code of practice provides a suggested best practice for all reporting entities conducting name and date of birth identity verification on customers (that are natural persons) they have assessed to be low to medium risk. Identification involves obtaining from the customer a range of information about him or her ("identity information"). Verification involves confirming some of that information against documents, data or information obtained from a reliable and independent source.

Under section 11 of the AML/CFT Act a reporting entity must conduct customer due diligence on a customer; a beneficial owner of a customer; and any person acting on behalf of a customer. In this code of practice customer refers to all natural persons that fall within these categories assessed by reporting entities as low to medium risk (that is, sections 11(1)(a) – (c)).

This code of practice provides for two ways of conducting identity verification, via documentary verification and electronic verification (Parts 1 and 3 of the code). Part 2

of the code provides for the certification of documents. This allows for non face-to-face documentary verification.

Reporting entities must have regard to privacy under all Parts (1-3) of this code of practice, including whether the management and provision of information is consistent with the principles of the Privacy Act 1993.

The Act also requires that reporting entities conduct verification of a customer's address using documents, data or information issued by a reliable and independent source.[1] While this code of practice does not intend to prescribe how to do so, reporting entities must determine an appropriate method for verifying a customer's address from a reliable and independent source.

For the avoidance of doubt, address verification must be carried out in addition to the name and date of birth identity verification requirements set out in Part 1 (documentary identity verification) of this code of practice in order to meet the obligations in sections 13, 16 and 24 of the Act. In order to rely on this code of practice for electronic identity verification of a customer's name and date of birth reporting entities must conduct address verification in accordance with Part 3 of this code (electronic identity verification).

This code of practice does not apply to the identity verification of customers (that are natural persons) assessed by reporting entities to be high risk. Increased or more sophisticated measures should be applied for high risk customers.

Legal obligations relating to identity verification

Subpart 1 of Part 2 of the AML/CFT Act outlines customer due diligence requirements. A reporting entity's AML/CFT programme, established under sections 56 – 57 of the Act, must include adequate and effective policies, procedures and controls for complying with customer due diligence requirements.

A reporting entity must base its AML/CFT programme, including its assessment of risk for the purpose of customer due diligence, on the AML/CFT risk assessment undertaken in accordance with section 58.

This code of practice applies to customers (that are natural persons) assessed by reporting entities as low to medium risk, for the verification of name and date of birth as required by:

i. Section 16 – standard customer due diligence: verification of identity requirements
ii. Section 20 – simplified customer due diligence: verification of identity requirements
iii. Section 24 – enhanced customer due diligence: verification of identity requirements[2]
iv. Section 28 – wire transfers: verification of identity requirements.

The Financial Markets Authority, Reserve Bank of New Zealand and the Department of Internal Affairs will consider reporting entities who comply with this code of practice

[1] Sections 13, 16 and 24 of the Act

[2] The Act requires enhanced due diligence in certain circumstances, however the Act does not predetermine that customers for whom enhanced due diligence is required be assessed as high risk. For example a politically exposed person might be assessed as a low to medium risk customer, but will always be subject to enhanced due diligence as required by section 24.

to have met their obligations to verify name and date of birth under sections 16, 20, 24 and 28 of the AML/CFT Act for low to medium risk customers (that are natural persons).

Note: A word or expression used in this code of practice has the same meaning as in the AML/CFT Act (see section 34 of the Interpretation Act 1999).

What will you find in this code of practice?
This code of practice covers all reporting entities in all AML/CFT sectors.

This code of practice is in three parts

PART 1: DOCUMENTARY IDENTITY VERIFICATION

PART 2: DOCUMENT CERTIFICATION

PART 3: ELECTRONIC IDENTITY VERIFICATION

PART 1: DOCUMENTARY IDENTITY VERIFICATION

In order to conduct documentary verification of a customer's name and date of birth, the following is required:

1. One form of the following primary photographic identification:

a) New Zealand passport
b) New Zealand certificate of identity issued under the Passports Act 1992
c) New Zealand certificate of identity issued under the Immigration New Zealand Operational Manual that is published under section 25 of the Immigration Act 2009
d) New Zealand refugee travel document issued under the Passports Act 1992
e) emergency travel document issued under the Passports Act 1992
f) New Zealand firearms licence
g) overseas passport or a similar document issued for the purpose of international travel which:

   i. contains the name, date of birth, a photograph and the signature of the person in whose name the document is issued; and
   ii. is issued by a foreign government, the United Nations or an agency of the United Nations.

h) a national identity card issued for the purpose of identification, that:

   i. contains the name, date of birth, a photograph and the signature of the person in whose name the document is issued; and
   ii. is issued by a foreign government, the United Nations or an agency of the United Nations.

OR

2. One form of the following primary non-photographic identification:

a) New Zealand full birth certificate
b) certificate of New Zealand citizenship issued under the Citizenship Act 1977
c) a citizenship certificate issued by a foreign government
d) a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations

in combination with a secondary or supporting form of photographic identification, for example:

e) New Zealand driver licence
f) 18+ Card
g) valid and current international driving permit as defined in clause 88(1)(b) of the Land Transport (Driver Licensing) Rule 1999.

Clauses 2 (e) – (g) are not an exhaustive list of secondary or supporting forms of photographic identification that may be acceptable. Reporting entities must ensure they are satisfied that any secondary or supporting photographic identification they accept is issued by an independent and reliable source.

Confirmation that the information presented (in the secondary or supporting form of photographic identification) is consistent with the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995 or the Citizenship Act 1977 by the Department of Internal Affairs can be substituted for the primary non-photographic identification required in this clause.

OR

3. The New Zealand driver licence and, in addition, one of the following:

a) confirmation that the information presented on the driver licence is consistent with records held in the National Register of driver licences
b) confirmation that the identity information presented on the New Zealand driver licence is consistent with the records held by a reliable and independent source (for example the information that is recorded for the purposes of the Births, Deaths, Marriages, and Relationships Registration Act 1995, the Citizenship Act 1977, or the Passports Act 1992 by the Department of Internal Affairs)
c) a document issued by a registered bank that contains the person's name and signature, for example a credit card, debit card or eftpos card
d) a bank statement issued by a registered bank to the person in the 12 months immediately preceding the date of the application
e) a document issued by a government agency that contains the person's name and signature, for example a SuperGold Card as defined in the Social Security (SuperGold Card) Regulations 2007
f) a statement issued by a government agency to the person in the 12 months immediately preceding the date of the application, for example a statement from the Inland Revenue Department.

Note: Regulation 13(3) of the Health Entitlement Cards Regulations 1993 places strict restrictions on those who can legally demand or request a community services card as a form of identification. Reporting entities may accept a community services card under clause 2(e) if the customer offers it; however they cannot request it.

4. In order to comply with this code, the reporting entity must have appropriate exception handling procedures in place, for circumstances when a customer demonstrates that they are unable to satisfy the requirements in 1 to 3 above.

5. Reporting entities must check the person's details against their customer records, to ensure that no other person has presented the same identity information or documents.

6. Where documents are provided in a language that is not understood by the person carrying out the verification an English translation must be provided.

7. In all instances where documentary verification is being used a reporting entity should verify the identity of the customer:

a) face to face; or by
b) copies of documents provided that are certified by a trusted referee (see below for certification requirements).

PART 2: DOCUMENT CERTIFICATION

8. A trusted referee must be at least 16 years of age and one of the following:

a) Commonwealth representative (as defined in the Oaths and Declarations Act 1957)
b) An employee of the Police who holds the office of constable (as defined in section 4 of the Policing Act 2008)
c) Justice of the peace
d) Registered medical doctor
e) Kaumātua
f) Registered teacher
g) Minister of religion
h) Lawyer (as defined in the Lawyers and Conveyancers Act 2006)
i) Notary public
j) New Zealand Honorary consul
k) Member of Parliament
l) Chartered accountant (within the meaning of section 19 of the New Zealand Institute of Chartered Accountants Act 1996).

9. In addition, the trusted referee must not be:

a) related to the customer; for example, a trusted referee cannot be their parent, child, brother, sister, aunt, uncle or cousin
b) the spouse or partner of the customer
c) a person who lives at the same address as the customer.

10. The trusted referee must sight the original documentary identification, and make a statement to the effect that the documents provided are a true copy and represent the identity of the named individual (link to the presenter).

11. Certification must include the name, occupation and signature of the trusted referee and the date of certification.

12. Certification must have been carried out in the three months preceding the presentation of the copied documents.

PART 3: ELECTRONIC IDENTITY VERIFICATION

13. In order to conduct electronic identity verification of a customer's name and date of birth a reporting entity must;

a) verify the customer's name from at least two reliable and independent electronic sources;
b) verify the customer's date of birth from at least one reliable and independent electronic source; and
c) verify the customer's address from at least one reliable and independent electronic source.

14. Reporting entities must check the person's details against their customer records, to ensure that no other person has presented the same identity information or documents.

15. When determining what type of electronic sources will be considered reliable and independent reporting entities must have regard to:

a) accuracy (how up-to-date is the information and what are the error rates and matching parameters);
b) security;
c) privacy (including whether the management and provision of the information is consistent with the principles of the Privacy Act 1993);
d) method of information collection;
e) whether the electronic source has incorporated a mechanism to determine the customer can be linked to the claimed identity (whether biometrically or otherwise);
f) whether the information is maintained by a government body or pursuant to legislation; and
g) whether the information has been additionally verified from another reliable and independent source.

16. Reporting entities that use electronic identity verification methods must include information in their AML/CFT compliance programme that describes:

a) the forms of electronic identity verification methods that are considered reliable and independent and in what circumstances they will be used for the purposes of identity verification;
b) how the methods have regard to the matters described in clause 15; and
c) any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

Note: Nothing in this code of practice prevents a reporting entity from obtaining multi-source verification from a single provider, so long as they are satisfied that the requirements in Part 3 are complied with.