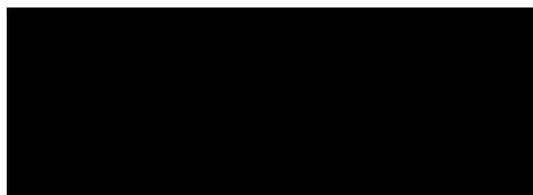


AML / CFT

Anti-money laundering and countering financing of terrorism

Amended Identity Verification Code of Practice 2013



INTERNAL AFFAIRS



Te Tari Taiwhenua

Amended Identity Verification Code of Practice 2013

(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 (the code) 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 amended code of practice was approved by notice in the New Zealand Gazette on the 10th day of October 2013.

Introduction

The Identity Verification Code of Practice 2013 Explanatory Note provides background information and resources and should be read in conjunction with this code.

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) that have been 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 falling within 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.

The AML/CFT 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 This code of practice does not prescribe the way in which reporting entities can fulfil this obligation.

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.

¹ Sections 13, 16 and 24 of the Act

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 requirements²
- 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 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:

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.

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 and a photograph of the person in whose name the document is issued and their signature or other biometric measure included where relevant ; 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 rule 88(1)(b) of the [Land Transport \(Driver Licensing\) Rule 1999](#) and a licence from another country with a translation.

Points 2 (e) – (g) above 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 independent and reliable.

Confirmation that the identity information presented in the secondary or supporting form of photographic identification 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 or the Citizenship Act 1977 by the Department of Internal Affairs can be substituted for the primary non-photographic identification required in points 2(a)-(d).

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 point 3(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 have a process in place to check that no other person with the same or similar names 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. In New Zealand 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) Member of the police
 - c) Justice of the peace
 - d) Registered medical doctor
 - e) Kaumātua (as verified through a reputable source)
 - 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)
 - m) A person who has the legal authority to take statutory declarations or the equivalent in New Zealand

Certification when overseas

9. When certification occurs overseas, copies of international identification provided by a customer resident overseas must be certified by a person authorised by law in that country to take statutory declarations or equivalent in the customer's country.
10. 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
 - d) a person involved in the transaction or business requiring the certification.
11. 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).
12. Certification must include the name, signature, and the date of certification. The trusted referee must specify their capacity to act as a trusted referee from sections 8(a)-(m) above.
13. Certification must have been carried out in the three months preceding the presentation of the copied documents.

PART 3: ELECTRONIC IDENTITY VERIFICATION

14. An electronic identity is a record kept in electronic form that contains authenticated core identity information about an individual. Electronic identity

verification is using that record to verify an individual's identity when a reporting entity is conducting customer due diligence.

15. 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 either:
 - a. a single independent electronic source that is able to verify an individual's identity to a high level of confidence; or
 - b. at least two independent and reliable matching electronic sources.
 - b) verify the customer's date of birth from at least one reliable and independent electronic source.
16. 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.
17. 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 Information Privacy Principles 5 to 11 in section 6 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.
18. 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 17; 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.