# AML / CFT

**Anti-money laundering and countering financing of terrorism**

# Identity Verification Code of Practice – Explanatory Note

**Updated in December 2017**

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

RESERVE BANK
OF NEW ZEALAND
*TE PŪTEA MATUA*

Te Tari Taiwhenua
Internal Affairs

# Explanatory Note

1. This Explanatory Note should be read in conjunction with the Amended Identity Verification Code of Practice 2013. This note replaces the previous Explanatory Note that was published in October 2013.

2. The Amended Identity Verification Code of Practice 2013 (the code) clarified requirements for electronic identity verification following the implementation of the Electronic Identity Verification Act 2012 and the Identity Information Confirmation Act 2012. It replaced the previous Identity Verification Code of Practice 2011.

3. This Explanatory Note provides further clarification to reporting entities that seek to comply with Part 3 of the code by using electronic identity verification.

## Electronic Verification

4. Electronic verification is considered to be where a customer's identity is verified remotely or non-face-to-face.

5. Electronic verification has two key components, firstly confirmation of identity information via an electronic source(s) and secondly matching the person you are dealing with to the identity that they are claiming (*i.e. are they the same person)?* Both components must be satisfied.

6. The electronic source is the underlying repository where the authenticated core identity information is held and against which an individual's identity is to be verified. In most circumstances, this is going to be information that is maintained by a government body or pursuant to legislation.

7. For electronic identity verification, it is important to remember that the electronic source is not any of the following:
   - The person that the reporting entity is dealing with online who provides their biographical information,
   - A selfie photo or video
   - An uploaded image of their identity document(s)
   - The email, application or internet platform that the reporting entity uses to receive this information or documents
   - The third party provider that a reporting entity uses to conduct its online electronic verification.

## Using a single independent source

8. The code reflects that a reporting entity can satisfy electronic identity verification requirements from a single electronic source that is able to verify an individual's identity to a high level of confidence. Only an electronic source that incorporates biometric information or information which provides a level of confidence equal to biometric information enables an individual's identity to be verified to a high level of confidence.

9. Biometric information includes measurements of an individual's physical characteristics that can be recorded and used for comparison and automated recognition of that individual *e.g. photographs, iris structure or fingerprint information such as arch, whorl and loop types*.

**Using two reliable and independent matching sources**

10. The code also allows a reporting entity to verify an individual's identity from at least two electronic sources which must be:
    - Reliable, and
    - Independent, and
    - Match each other. [1]

11. Where two "reliable and independent" sources are used and they match each other, the "high level of confidence" required of a single independent source is not required.

12. Where two matching reliable and independent electronic sources are to be used, a reporting entity must still have regard to whether the electronic sources include a mechanism to determine if the customer can be linked to the claimed identity.

13. If the electronic sources do not contain this mechanism, additional or supplementary measures must be used to ensure the person that the reporting entity is dealing with is the genuine holder of the identity they are claiming to be.

**Additional measures required**

14. Clause 17(e) of the code requires a reporting entity to consider whether the electronic source(s) has incorporated a mechanism to determine whether the customer can be linked to their claimed identity (whether biometrically or otherwise). If the electronic source(s) does not have such a mechanism, or it is not robust enough, then a reporting entity is able to adopt additional measures that will be used to supplement it, or to otherwise mitigate any deficiencies in the process.

15. Some examples of additional measures include the following:

    - Require the first credit into the customer's account or facility to be received from an account/facility held at another New Zealand reporting entity in the customer's name.

    - Issue a letter that contains a unique reference/identifier to the customer's address that has been verified by a reliable and independent source. The letter/unique reference number must be returned to the reporting entity before the customer's account or facility is fully operational *e.g. before any withdrawals/debits can be conducted*.

[1] Note that it is possible for a reporting entity to verify an individual's identity from two or more "reliable and independent" sources but via a single third party provider.

- Robust steps to confirm the authenticity of any identification document electronically provided by the customer. This should ensure that both the document belongs to the customer and that it has not been forged, altered or tampered with in any way *e.g. the original photo on the identification document is replaced*.

- Phone the customer on a number that has been verified by a reliable and independent source before the customer's account or facility is fully operational *e.g. before any withdrawals/debits can be conducted*.

- Robust security type questions based on reliable and independent information obtained about a person's social or financial footprint. This information should not be publicly available or easily obtained.

**Inclusion with AML/CFT Programme**

16. Reporting entities that utilise electronic verification must clearly describe in their AML/CFT Programme how all the relevant criteria within the code are satisfied. This includes any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

**Customers who established a business relationship before 30 June 2013**

17. Electronic sources could also be used to verify identity information for existing customers who established a business relationship with a reporting entity before 30 June 2013. Requirements in the code will still apply.

**About codes of practice**

18. Codes of practice are intended to provide a statement of practice to assist reporting entities to comply with certain Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (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.

19. 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.

20. 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.

Resources for the Amended Identification Verification Code of Practice 2013:

- Evidence of Identity Standard available on the Department of Internal Affairs' website
- Te Kāhui Māngai, a directory of Iwi and Māori organisations available on Te Puni Kokiri website.