

AML/CFT

Anti-money laundering and countering financing of terrorism

Identity Verification Code of Practice 2026



INTRODUCTION

The Identity Verification Code of Practice (**code of practice** or **code**) was approved by notice in the New Zealand Gazette on the 28th day of May 2026 by the Minister of Internal Affairs under section 64 of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the **Act**).

This code commences on 1 July 2026, excluding paragraphs 1.4.3 to 1.4.5 (inclusive) which commence on 1 July 2027, and remains in effect until replaced by another code approved as required by section 64 of the Act.

I. What is this code of practice for?

This code of practice provides a suggested best practice for all reporting entities conducting full name and date of birth identity verification on their customers (that are natural persons), beneficial owners of customers and persons acting on behalf of customers.

The requirements to identify these persons are part of the customer due diligence (**CDD**) requirements under section 11(1)(a)-(c) of the Act.

CDD involves obtaining certain information about the customer (**identity information**). Some of this information must be verified on the basis of documents, data or information from a reliable and independent source.

II. What is contained in this code of practice?

This code of practice is in three parts:

- Part 1: Identity Verification Pathways
 - 1.1: Face-to-face verification using physical documents
 - 1.2: Verification through the Digital Identity Services Trust Framework
 - 1.3: Other Electronic Identity Verification methods
 - 1.4: Certified copies of identity documents
- Part 2: Identity Verification of eligible Beneficial Owners and Persons Acting on Behalf of Customers
- Part 3: Other Conditions

The code of practice applies to full name and date of birth verification as required by:

- Section 13 – relating to verification of name and date of birth of a natural person;
- Section 16 – standard CDD: verification of identity requirements;
- Section 20 – simplified CDD: verification of identity requirements;¹
- Section 24 – enhanced CDD: verification of identity requirements; and
- Section 28 – wire transfers: verification of identity requirements.

¹ Note that the requirements of section 20 of the Act are included in the code at the time of publication.

The name and date of birth of a customer who is a natural person must be verified from one of the pathways established in subpart 1.1, 1.2, 1.3, and 1.4 of the code.²

The name and date of birth of a beneficial owner or person acting on behalf of a customer must be verified:

- from one of the pathways established in subpart 1.1, 1.2, 1.3, and 1.4 of the code; or
- for eligible beneficial owners or persons acting on behalf, in accordance with Part 2 of the code.

The AML/CFT Supervisor(s) 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 Act for natural persons.

This code of practice does not contain provisions for the following obligations under the Act:

- verification of name and date of birth of a customer if required subsequent to the establishment of a business relationship;³
- the steps required to identify the persons that meet the definition of beneficial owner (prior to verifying their name and date of birth);
- the risk-rating of customers; or
- record keeping requirements.

III. Interpreting this code

Regulations require a reporting entity to risk-rate a new customer.⁴ This code of practice adopts descriptors for risk ratings of “low”, “medium” and “high”. If a reporting entity uses another descriptor (for example “medium-low” and “medium-high” or a numerical score), this should be calibrated for the purpose of applying the code to align with a low, medium and high rating scale.

A word or expression used in this code of practice has the same meaning as in the Act (see section 20 of the [Legislation Act 2019](#)).

Examples provided in the code are not exhaustive and do not limit the provisions of the code which they relate to (see section 23 of the [Legislation Act 2019](#)).

Footnotes included in this document do not form part of the code of practice but instead provide further context or relevant information to assist reporting entities.

IV. New Zealand Identification Standards

The code of practice adopts the “Information Assurance” and “Binding Assurance” components of the [NZ Identification Standards](#):

² This includes circumstances when two or more people are jointly a customer (such as a joint bank account).

³ For example, as part of ongoing CDD or if enhanced CDD under section 22(1)(c) or (d) of the Act is triggered.

⁴ As required by Regulation 12AC of the AML/CFT (Requirements and Compliance) Regulations 2011.

- **Information Assurance:** is the robustness of the process to establish the quality and accuracy of the person's identity.
- **Binding Assurance:** is the robustness of the process to bind the person being dealt with to that identity, sometimes referred to as the "linking mechanism".

V. Legal effect of a code of practice

The legal effect of a code of practice is described in section 67 of the Act.

Complying with the code of practice is not mandatory. The AML/CFT system allows for flexibility and scope for innovation because reporting entities can opt out of a code of practice. However, if fully complied with, the code of practice operates as a 'safe harbour'. This means that in the event enforcement action is taken, a court must have regard to this code of practice in determining whether a reporting entity is compliant with its obligations relating to verification of a person's name and date of birth.

If a reporting entity decides not to comply with the code of practice, it must comply with the obligation to verify a person's name and date of birth by some other equally effective means. 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 of practice and intends to satisfy its obligations by some other equally effective means.

This code of practice replaces the Amended Identity Verification Code of Practice 2013 that was approved by notice in the New Zealand Gazette on 10 October 2013.

This code of practice covers all reporting entities under the Act.

PART 1: IDENTITY VERIFICATION PATHWAYS

1.1 Face-to-face verification using physical documents

Information Assurance

1.1.1 A customer's full name and date of birth must be verified from either—

(a) **one form of the following primary photographic identification:**

- (i) New Zealand passport;
- (ii) New Zealand certificate of identity issued under the [Passports Act 1992](#);
- (iii) New Zealand certificate of identity issued under the Immigration New Zealand Operational Manual that is published under section 25 of the [Immigration Act 2009](#);
- (iv) New Zealand refugee travel document issued under the [Passports Act 1992](#);
- (v) emergency travel document issued under the [Passports Act 1992](#);
- (vi) New Zealand firearms licence;
- (vii) overseas passport or a similar document issued for the purpose of international travel which—
 - (A) contains the name, date of birth and a photograph of the person in whose name the document is issued; and
 - (B) is issued by a foreign government, the United Nations or an agency of the United Nations;
- (viii) a national identity card issued for the purpose of identification, that—
 - (A) 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
 - (B) is issued by a foreign government, the United Nations or an agency of the United Nations;

OR

(b) **one form of the following primary non-photographic identification:**

- (i) New Zealand birth certificate;⁵
- (ii) New Zealand citizenship certificate issued under the [Citizenship Act 1977](#);
- (iii) a citizenship certificate issued by a foreign government;

⁵ There is no requirement to verify a person's sex assigned at birth. A customer has the right to redact any details from their birth certificate that are not required to be collected for a lawful purpose, and such a birth certificate is acceptable under the code.

- (iv) 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:⁶

- (v) New Zealand driver licence;⁷
- (vi) Kiwi Access Card / 18+ Card;
- (vii) 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;
- (viii) a SuperGold Card (with photograph) as defined in the [Social Security Regulations 2018](#); or
- (ix) a Total Mobility card issued by a regional council in New Zealand, Auckland Transport, or a council approved disability agency;

OR

- (c) **a New Zealand driver licence** and, in addition, one of the following:
 - (i) confirmation that the information presented on the driver licence is consistent with records held in the NZ Driver Licence Register;⁸
 - (ii) 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 2021](#), the [Citizenship Act 1977](#), or the [Passports Act 1992](#) by the Department of Internal Affairs);
 - (iii) a document issued by a registered bank that contains the person's name, for example a credit card,⁹ debit card or eftpos card;
 - (iv) a bank statement issued by a registered bank to the person in the 12 months immediately preceding the date of the application;
 - (v) a document issued by a government agency that contains the person's name and signature,¹⁰ for example a SuperGold Card as defined in the [Social Security Regulations 2018](#);
 - (vi) 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; or

⁶ Points (v) – (ix) are not an exhaustive list of secondary or supporting forms of photographic identification. Other reliable and independent secondary or supporting photographic identification may be accepted.

⁷ This includes New Zealand driving licences issued electronically by NZ Transport Agency Waka Kotahi (NZTA).

⁸ This could be correspondence in writing from NZTA or use of an API or intermediary to verify driver licence details from the NZTA website.

⁹ For reporting entities that handle credit cards, the Payment Card Industry Data Security Standard (PCI DSS) provides a baseline of technical and operational requirements designed to protect payment account data.

¹⁰ 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 (c)(v) if the customer offers it; however, they cannot request it.

- (vii) a Total Mobility card issued by a regional council in New Zealand, Auckland Transport or a council approved disability agency.

1.1.2 All documents must be valid.¹¹

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

Binding Assurance

1.1.4 The photograph on the identity document must be visually compared to the customer that presents it to establish the likeness.¹²

1.2 Verification through the Digital Identity Services Trust Framework

1.2.1 Verification of a customer's name and date of birth through an accredited Digital Identity Services Trust Framework (**DISTF**) service may be conducted in person or online.

Information and Binding Assurance

1.2.2 A customer's full name and date of birth must be verified from a digital identity credential or service that is either—

(a) For verification in person or online—

- (i) issued by a digital identity service accredited by the DISTF;
- (ii) provides the customer's full name and date of birth to a Strong Plus Level of Information Assurance; and
- (iii) provides the customer's full name and date of birth to a Strong Plus Level of Binding Assurance:

OR

(b) For verification in person only—

- (i) issued by a digital identity service accredited by the DISTF;
- (ii) provides the customer's full name and date of birth to a Standard Plus Level of Information Assurance;
- (iii) provides the customer's full name and date of birth to a Standard Plus Level of Binding Assurance; and
- (iv) is supported by one of the primary non-photographic identification documents listed in paragraph 1.1.1(b)(i) through (iv) above.

¹¹ Note that as part of exception handling procedures under the code, an expired document could be accepted.

¹² This does not introduce an obligation to record that the visual comparison has been made, noting that making a visual comparison should be part of a reporting entity's procedures.

1.3 Other Electronic Identity Verification methods

- 1.3.1 Other electronic identity verification (**EIV**) methods for the purposes of the code may be used where a customer's name and date of birth is verified remotely (i.e. non-face-to-face) from an electronic source.
- 1.3.2 An electronic source is the underlying database or record where authenticated core identity information is held, and against which the customer's full name and date of birth is verified. The electronic source must be reliable and independent.
- 1.3.3 A customer's full name and date of birth may be verified from—
- (a) a single electronic source that provides both information assurance and binding assurance; or
 - (b) an electronic source that provides information assurance in combination with a separate linking mechanism that provides binding assurance.
- 1.3.4 To comply with the code, one of the following options (a) to (e) must be used:

Information and Binding Assurance

- (a) **a verified RealMe identity**;¹³

Information Assurance

- (b) **the DIA Confirmation Service**;
- (c) **a reliable non-New Zealand electronic source maintained by an overseas government body**, that is an electronic source containing reliable authenticated identity information. A reporting entity must consider each of the following to determine whether the electronic source contains reliable authenticated information:
 - (i) the method of information collection;
 - (ii) the quality and accuracy of the information;
 - (iii) security and privacy (including whether the management and provision of the information is consistent with the Information Privacy Principles 5 to 11 in section 22 of the [Privacy Act 2020](#)); and
 - (iv) the level of country risk;
- (d) **an embedded e-passport microchip in a customer's New Zealand passport or overseas passport**.¹⁴ The authenticity and integrity of the information on the e-passport microchip must be validated using the public key of the issuing state, including that it was issued by the given country and has not been tampered with; or

¹³ A verified RealMe identity is a single electronic source able to verify a customer's name and date of birth with a high level of confidence. It incorporates biometric verification providing Binding Assurance of a person to their claimed identity.

¹⁴ As described in paragraph 1.1.1(a)(vii) of the code.

- (e) **the NZ Transport Agency Waka Kotahi Driver Check.** When using this option, the customer's name must be verified from a second reliable and independent electronic source. For example:
 - (i) Credit Bureau;
 - (ii) Companies Office;
 - (iii) Land Registry (LINZ); or
 - (iv) vehicle registration (NZTA).

Binding Assurance

- 1.3.5 To comply with the code, options (b) to (e) above must be combined with a separate linking mechanism that provides binding assurance that the person being dealt with remotely is the genuine holder of the claimed identity.
- 1.3.6 Examples of separate linking mechanisms that provide binding assurance include:
 - (a) **use of EIV technology:**¹⁵ to ensure the authenticity of any identification document electronically provided by the customer. This process must utilise robust facial recognition software (including a liveness test) to bind the person being dealt with to the image on the identity document, and to ensure the document has not been forged, altered or tampered with;
 - (b) **first payment:** requiring the first credit into the customer's account or facility to be received from an account/facility held in the customer's name at a New Zealand registered bank; or
 - (c) **in person visit:** requiring the customer to subsequently physically visit the reporting entity for the original identity documents to be sighted (in accordance with subpart 1.1 above).¹⁶

1.4 Certified copies of identity documents

- 1.4.1 Subpart 1.4 commences on 1 July 2026, with the exception of paragraphs 1.4.3, 1.4.4, and 1.4.5 which commence on 1 July 2027.
- 1.4.2 A reporting entity may accept a certified copy of an original identity document.¹⁷
- 1.4.3 A reporting entity may receive a certified copy in person, by post or other means of delivery, including electronically.
- 1.4.4 A reporting entity must incorporate procedures, policies and controls that provide enhanced assurance that the person being dealt with is the genuine holder of the

¹⁵ This may include use of a third-party EIV provider. Note the supervisors do not consider that video conferencing technology involving the customer holding up a copy of their identity document can itself satisfy this requirement.

¹⁶ This may utilise the delayed verification provisions of the Act, including transaction limits, account monitoring (or other appropriate risk management procedures) until such time as the in-person verification has occurred. Note this also aligns with subpart 1.1 of the code.

¹⁷ These requirements for certified copies do not apply to a reporting entity's own processes for recording that original identity documents have been sighted, including when using an agent under section 34 of the Act. Nor do these requirements apply to circumstances when another reporting entity is being relied on to conduct CDD under sections 32-33 of the Act. (These obligations of the Act are not covered in this code of practice).

claimed identity¹⁸ where there are reasonable grounds for a concern that a copy may not be genuine.¹⁹

- 1.4.5 Reasonable grounds for a concern that a copy may not be genuine will likely arise in situations where a customer also presents as a high money laundering or terrorism financing risk.

Information Assurance

- 1.4.6 To comply with the code—

- (a) certification must be carried out by a “trusted referee”;
- (b) certification must include—
 - (i) the trusted referee’s name and signature;
 - (ii) the trusted referee’s capacity to act as a trusted referee;
 - (iii) the date of the certification; and
 - (iv) a statement to the effect that the certified copy is a true copy of the original document;
- (c) certification must have been carried out in the twelve months preceding presentation of the certified copy; and
- (d) the identity document (or combination of identity documents) for which a certified copy is received must meet the requirements of paragraphs 1.1.1 to 1.1.3.

Binding Assurance

- 1.4.7 To comply with the code—

- (a) the photograph on the certified copy must be clearly visible; and
- (b) either:
 - (i) for certified copies presented face to face, the photograph on the certified copy of the identity document must be visually compared to the person that presents it to establish the likeness; or
 - (ii) for certified copies provided through other means, the certified copy must include a statement from the trusted referee to the effect that the document provided represents the identity of the named individual.

Trusted referees

- 1.4.8 In New Zealand a trusted referee must be at least 16 years of age and one of the following:

¹⁸ Examples may include but are not limited to: checking a register to confirm the ability of the person to be a trusted referee, contacting the trusted referee to confirm they certified the document, or requiring original “wet ink” copies to be submitted.

¹⁹ Examples may include but are not limited to: inconsistencies in the certification, poor quality copies of documents, or evidence of tampering.

- (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) 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; or
- (n) Māori Land Court official (Registrar as defined by [Te Ture Whenua Maori Act 1993](#) or Regional Manager).

1.4.9 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; or
- (d) a person involved in the transaction or business requiring the certification.

Certification when overseas

1.4.10 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.

1.4.11 A reporting entity may accept an overseas certification without a statement from the person authorised by law that the document provided represents the identity of the named individual. A reporting entity that accepts an overseas certification without this statement must have appropriate risk-based procedures, policies and controls for alternative means for binding assurance.

PART 2: IDENTITY VERIFICATION OF ELIGIBLE BENEFICIAL OWNERS AND PERSONS ACTING ON BEHALF OF CUSTOMERS

- 2.1 For verification of name and date of birth of a beneficial owner and a person acting on behalf of a customer, the extent of the verification steps required is dependent on the level of risk associated with the customer.²⁰

Applying reduced verification steps

- 2.2 A natural person is **eligible** for reduced verification steps if they are a beneficial owner or person acting on behalf of a customer—
- (a) that is a legal person or a legal arrangement;
 - (b) that is rated as **Low** or **Medium** risk; and—
 - (i) that has two or more beneficial owners; or
 - (ii) for which simplified CDD under section 18(1) or (3) of the Act applies.
- 2.3 A beneficial owner or person acting on behalf of a customer who is not eligible under paragraph 2.2 above must be verified through one of the pathways in Part 1 of the code.
- 2.4 To comply with the code when verifying the identity of an eligible Beneficial Owner or Person Acting on Behalf of a Customer, a reporting entity must—
- (a) follow the requirements set out in Part 1; or
 - (b) apply appropriate reduced verification steps established in its AML/CFT programme. A reporting entity must still, accordingly to the level of risk involved, be satisfied it knows who the person is.²¹
- 2.5 In establishing reduced verification steps in its AML/CFT programme, a reporting entity must have appropriate risk-based procedures, policies and controls,²² which include—
- (a) what the reduced verification steps are; and
 - (b) the circumstances in which those reduced verification steps may be taken.
- 2.6 Reduced verification steps are **not** permitted in circumstances when there are grounds to report a suspicious activity.

²⁰ In accordance with section 16(1)(b) and (c) of the Act.

²¹ Examples of reduced verification steps may include but are not limited to: accepting a lesser standard of physical identity documents (to those in subpart 1.1), a lesser standard of assurance through an accredited DISTF service, accepting uncertified copies of documents by email and/or using video conferencing to link a person to their claimed identity.

²² Risk based procedures, policies and controls may include consideration of the information obtained regarding the beneficial owners and persons acting on behalf of customers and may consider any additional measures implemented to mitigate the risks associated with the reduced verification steps.

Certified copies of documents for eligible Beneficial Owners or Persons Acting on Behalf

- 2.7 When verifying the identity of an eligible Beneficial Owner or Person Acting on Behalf of a Customer, the condition in paragraph 1.4.9(d) above does not apply if the certifier is employed by the customer and is—
- (a) a lawyer as defined in the [Lawyers and Conveyancers Act 2006](#); or
 - (b) a person authorised by law in another jurisdiction to act in a capacity equivalent to a lawyer as defined in the [Lawyers and Conveyancers Act 2006](#).

PART 3: OTHER CONDITIONS

- 3.1 A reporting entity must have a process in place to check that no other person has presented the same identity information.

Originators of wire transfers

- 3.2 This code of practice applies to identity verification of an originator of a wire transfer (that is a natural person) as required under section 28 of the Act.
- 3.3 In most circumstances, the originator of a wire transfer is also a “customer” as defined in the Act.²³ The code does not require a reporting entity to verify the name and date of birth of an originator of a wire transfer if it has already done so (as part of conducting CDD under the Act on the person as a “customer”), unless there are reasonable grounds to doubt the adequacy or veracity of the identity verification previously conducted.²⁴

Exception handling procedures

- 3.4 To comply with the code, a reporting entity must have appropriate exception handling procedures in place, for circumstances when a person demonstrates they are unable to comply with the requirements of Parts 1 or 2 of the code.²⁵
- 3.5 A reporting entity’s exception handling procedures must have appropriate escalation procedures, policies and controls in place.²⁶
- 3.6 A reporting entity may maintain a standard process for common exceptions.
- 3.7 To support financial inclusion, a reporting entity may implement appropriate risk management procedures (such as transaction restrictions and additional account monitoring) alongside making an exception to the code.
- 3.8 Nothing in the code overrides the requirement to comply with section 37 of the Act.

AML/CFT programme

- 3.9 A reporting entity must include the procedures, policies and controls that they utilise to comply with the code of practice in their AML/CFT compliance programme.

²³ In a limited set of circumstances in the money or value transfer sector, the originator of a wire transfer may not be the reporting entity’s customer. Verification requirements in relation to the originator in these circumstances are not covered in this code.

²⁴ In accordance with section 11(4) of the Act. Note also that the code does not introduce a requirement to conduct CDD on an “existing customer” that is the originator of a wire transfer unless this is otherwise required by the Act or regulations.

²⁵ Examples of circumstances when exceptions may be appropriate include but are not limited to: financial inclusion reasons, children or young adults, vulnerable people, people with disabilities, or people advanced in age, that are unable to meet the code’s requirements.

²⁶ Examples of escalation procedures, policies and controls include but are not limited to: escalation to a second line reviewer, obtaining independent corroboration of a person’s identity or incorporating an interview with the person.

Version history

September 2011	Initial version
October 2013	Updated to include electronic identity verification from a single independent source providing a high level of confidence. Also, removal of address verification requirements from the code of practice.
May 2026	Publication of the Identity Verification Code of Practice 2026. This code replaces the 2013 code and includes: • Verification of high-risk customers. • Verification through an accredited Digital Identity Services Trust Framework service. • Clarification to the use of other electronic identity verification methods and certified copies of identity documents. In addition, the requirement that a person's name be verified from a second reliable and independent source has been removed if the DIA Confirmation Service is being used. Furthermore, verification requirements for beneficial owners and persons acting on behalf of the customer are now according to the level of risk.

Other resources for the Identity Verification Code of Practice 2026

- [Te Kāhui Māngai](#), a directory of Iwi and Māori organisations available on Te Puni Kokiri website.