2Shakes Identity Verification:

IDV Code of Practice 2026

This document provides details of how identity verification in 2Shakes meets the New Zealand Identity Verification Code of Practice 2026. The 2026 Code took effect on 1 July 2026. The information below is for New Zealand AML/CFT reporting entities to include or refer to in their own AML programmes. This information is also available on the 2Shakes website at https://2shakes.co.nz/IDVCOP

2Shakes Biometric Identity Verification fully meets NZ's IDV Code of Practice

From 1 July 2026, the Identity Verification Code of Practice outlines best practice for AML reporting entities. 2Shakes Biometric Identity Verification:

- Uses government databases as electronic sources that are reliable and independent to provide information assurance as per 1.3.4(b), 1.3.4(c), and 1.3.4(e).
- Is used in combination with a separate linking mechanism that provides binding assurance as per 1.3.6(a).

Biometric Identity Verification is the recommended option.

It fully meets the Code of Practice and is easy and efficient to do. 2Shakes defaults to Biometric Identity Verification as it also meets other government ID requirements. For example, it meets Inland Revenue's operational statement OS 25/3 for tax agents or registered bookkeepers to identify clients they need authority to act for. That is why Biometric IDV is the 2Shakes default option when AML CDD or IR authorities apply.

Biometric Identity Verification for the AML/CFT Act

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 Anti-Money Laundering and Countering Financing of Terrorism Act 2009 for natural persons.

How 2Shakes meets the NZ IDV Code of Practice 2026 — clause by clause

The information below is for the benefit of New Zealand AML/CFT reporting entities to include or refer to in their own AML programme.

The Identity Verification Code of Practice 2026 provides four pathways for identity verification, and 2Shakes Biometric Identity Verification fully complies with pathway 1.3, *Other Electronic Identity Verification Methods*.

How 2Shakes meets the clauses in this pathway is described below:

- **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.*
  2Shakes Biometric Identity Verification electronically verifies the customer's name and date of birth remotely to meet these requirements.
- **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.*
  2Shakes only uses highly trusted government databases as electronic sources that are 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.*
  2Shakes uses 1.3.3(b) electronic sources that provide 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.*
  2Shakes uses options (b), (c), and (e), as applicable.
  - **1.3.4(b)** *the DIA Confirmation Service*;
    2Shakes verifies NZ passport data against the DIA confirmation service.
  - **1.3.4(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;
2Shakes uses the Australian Government's Document Verification Service (DVS) to verify Australian passport or driver licence data.

    - **1.3.4(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)*
    2Shakes uses the NZ Transport Agency Waka Kotahi Driver Check, along with Centrix Credit Bureau data, Companies Office (NZBN) data, and LINZ data.

- **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.*
2Shakes Biometric Identity Verification provides a linking mechanism that provides binding assurance.
- **1.3.6(a)** *Use of EIV technology: 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.*
2Shakes Biometric Identity Verification checks the authenticity of the document and utilises robust facial recognition software, including a liveness test, as per clause 1.3.6 requirements.

Politically Exposed Person and Sanctions Check

2Shakes Biometric Identity Verification also includes a Politically Exposed Person and Sanctions (PEP) check, as required under section 26 of the Act.

Remove old references

Any references to the old IDVCOP or explanatory note should now be replaced with this new Code of Practice.

Other IDV methods have additional requirements

2Shakes allows the selection and recording of other identity verification methods. It is important to ensure all requirements that apply under the Code of Practice are met. Depending on the method and circumstances, different additional requirements may apply. Some, but not all, examples are given below:

- Electronic IDV in 2Shakes requires you to record additional measures: either 1.3.6(b), first payment, or 1.3.6(c), in-person visit.
- Manual IDV face to face requires that you must meet the person at the same time they have their original identity documents with them. The Code outlines which document, or combination of documents, is acceptable as per 1.1.1.
- Manual IDV with a certified copy of an identity document requires the certifier to confirm that the person's likeness matches the photograph on the identity document, as per 1.4.7.
- For low-risk or medium-risk customers with either two or more beneficial owners, or under simplified CDD, you can establish a reduced verification process in your programme, as per Part 2.

Independent advice

Finally, you should always obtain independent expert and/or legal advice in relation to your AML programme and how you, as a reporting entity, comply with the legislation.

References

- DIA IDVCOP fact sheet
- AML/CFT Identity Verification Code of Practice 2026
- Anti-Money Laundering and Countering Financing of Terrorism Act 2009