

# Submission

to the

Department of Internal Affairs,  
Reserve Bank of New Zealand and  
Financial Markets Authority

on the

Discussion Paper: *Updating the  
Identity Verification Code of  
Practice*

19 January 2026



## About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.
2. The following seventeen registered banks in New Zealand are members of NZBA:
  - ANZ Bank New Zealand Limited
  - ASB Bank Limited
  - Bank of China (NZ) Limited
  - Bank of New Zealand
  - China Construction Bank (New Zealand) Limited
  - Citibank N.A.
  - The Co-operative Bank Limited
  - Heartland Bank Limited
  - The Hongkong and Shanghai Banking Corporation Limited
  - Industrial and Commercial Bank of China (New Zealand) Limited
  - JPMorgan Chase Bank N.A.
  - KB Kookmin Bank Auckland Branch
  - Kiwibank Limited
  - Rabobank New Zealand Limited
  - SBS Bank
  - TSB Bank Limited
  - Westpac New Zealand Limited

## Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable  
Deputy Chief Executive & General Counsel  
[antony.buick-constable@nzba.org.nz](mailto:antony.buick-constable@nzba.org.nz)

Sam Schuyt  
Policy Director & Legal Counsel  
[sam.schuyt@nzba.org.nz](mailto:sam.schuyt@nzba.org.nz)



## Introduction

4. NZBA welcomes the opportunity to provide feedback to the Department of Internal Affairs, Reserve Bank of New Zealand and Financial Markets Authority (together, the Supervisors) on their Discussion Paper: Updating the Identity Verification Code of Practice (**Consultation**).
5. We consider that a number of the proposed changes will provide welcome clarity, flexibility and streamlining of the Identity Verification Code of Practice (**IVCOP**) while still maintaining the necessary quality of verification and assurance.
6. However, we consider that other proposals will negatively impact customers through an increase in friction in the onboarding process. There could also be additional costs incurred through the certification process that further impact customer access.
7. Further, the proposals seem to be suited or directed at smaller reporting entities (**REs**) but cumbersome and problematic for larger REs. For REs that operate nationally, have multiple onboarding channels, have hundreds or thousands of staff involved in onboarding and rely on technology / systems to support onboarding and CDD obligations, many of the proposals are simply too cumbersome and onerous which, if implemented, will create friction in the onboarding process which, importantly, will ultimately impact customers.
8. We have structured the below submission in response to each proposal, with what we view as the two key proposals – Proposals 3 and 4 – addressed first. The balance of proposals are then addressed in order, where we have achieved an industry view.

## Proposal three: Document Certification

9. We understand the proposal is to clarify the ways in which a certified copy of an identity document can be used. However, as expanded upon below, we submit that the proposals are confusing, complicated and risk making the use of certified copies unworkable. They are also unnecessarily increasing the compliance burden and cost for both customers and REs.

### Physical attendance requirements

10. While we support clarity, we do not support the proposed 'clarification' of the circumstances under which certified copies can be used. This proposal would both unnecessarily introduce a heavy compliance burden on REs, as well as increasing barriers to accessing banking for customers. Part 2 of the IVCOP already establishes a workable, clear, controlled regime for certified copies.
11. Having to record why a customer cannot attend in person is onerous and cumbersome, and would also require technology changes to onboarding systems to capture the recorded reason. REs would also need to conduct assurance over their



decisions, and potentially remediate and offboard customers if they do not provide a response or valid reason.

12. Training staff on what is a valid reason for non-attendance would be challenging – for example, if a customer has broken their leg, would this be sufficient, or would a more permanent disability be required to reach the threshold? Similarly, would rural customers who face a long commute to reach a branch qualify for non-attendance?
  - 12.1. Following customer demand, many REs are transitioning to make more services available online.
  - 12.2. Instead, we submit that a certifier should be able to verify and certify through a video call.
13. While we support allowing certified copies as an option where ID documents are provided from overseas, the proposal disadvantages New Zealand-based customers without mitigating any appreciable AML/CFT risk. REs are already able to mandate that certain high-risk customer types must present in-person to be verified, which ensures the right level of binding assurance for the risk posed.

#### Form of certified copy

14. NZBA strongly opposes the proposed changes to only receive the original wet ink document or one that meets the requirements of the Contract and Commercial Law Act 2017 (**CCLA**). In our view, this will likely significantly reduce the utility of certifications.
15. Implementing it would be cumbersome and expensive for customers, will be operationally challenging for REs, will slow down the onboarding process and is generally a significant step backwards.
  - 15.1. Implementing it would mean certified copies would need to be couriered or provided in person, rather than emailed as is current practice. Many customers will not be happy or comfortable with posting certified ID documents due to the risks involved, and traditional post is an increasingly slow process that would impact the time taken to set up an account. Rural customers are likely to be particularly impacted by this requirement as they are often geographically distant from an REs physical premises.
  - 15.2. We understand from drop-in sessions with the Supervisors that part of the rationale behind this proposal is that the Supervisors' view scanned copies of certified documents as being more vulnerable to fraud than original "wet ink" copies.
  - 15.3. We disagree with this argument, and submit that fraud risk is not materially higher for scanned, certified documents. Both scanned and wet ink



documents have vulnerabilities; we would not characterise one as being inherently riskier than the other. Further, in our view the physical posting of original “wet ink” certified copies of documents can pose a higher risk of identity fraud if those documents are intercepted (which is a material risk in certain high-risk jurisdictions) than the fraud risk associated with accepting scanned certification copies for identification purposes.

- 15.4. Additionally, we note that fraud risk is relevant to all channels used for ID verification, and is actively managed by REs. Fraud risk should remain separate from the AML/CFT processes and the IVCOP.
  - 15.5. Requiring wet-ink certification is no longer operationally aligned with modern digital scanning, storage, or remote onboarding practices. Wet-ink originals offer no increased assurance once scanned and stored electronically. We note that the acceptance of certified soft copies is in line with international practice and current domestic legislation.
  - 15.6. Overall, we note these proposals run counter to the Reserve Bank of New Zealand’s financial inclusion programme, for example its ongoing work to improve access to bank accounts, by making it more difficult for customers to provide the required information for onboarding, or to complete a one-off transaction such as evidencing they are the executor of a deceased estate.
  - 15.7. We also note that this proposal may create inconsistencies with the recommendation of the Finance and Expenditure Committee to remove AML/CFT road-blocks for Māori land trusts, as these trusts can have a number of individuals that need to be verified.<sup>1</sup>
16. In relation to s 266 of the CCLA, we note this provision is ambiguous, making it unclear how a RE can demonstrate compliance.

#### Certification requirements

- 17. NZBA supports the removal of the requirement for trusted referees to certify that the ID documents are a true likeness of the individual. We note that most trusted referees in New Zealand now include “true likeness” as part of their certifications, so it is less of a problem than it has been historically. However, it is not commonly used overseas which presents a challenge for international customers.
- 18. However, we note that the proposed “linking mechanism” may unintentionally increase compliance requirements for a RE and customers in situations where a trusted referee will not certify the identity of the customer.

---

<sup>1</sup> See the Finance and Expenditure Committee’s [Inquiry into banking competition](#), Recommendation 17 (August 2025).



- 18.1. The use of delayed electronic identity verification (**EIV**) methods will only be beneficial in instances where a passport or driver's licence is being utilised. This also does not appear to provide a link to the claimed identity as these measures will only confirm that the document exists, but will not confirm that the identity belongs to the customer.
- 18.2. The benefit of this provision appears to be limited because if EIV options were available and could be utilised, it is likely that these would be utilised in the first instance rather than following the certification process.
- 18.3. As noted above, the removal of "likeness" certification would primarily benefit situations involving international trusted referees. The use cases of EIV do not solve this issue.
- 18.4. From a customer's perspective, it is complex and time-consuming to obtain certified copies of their document, and subsequently being required to go through the electronic verification process.
- 18.5. Please refer to our comments in response to Proposal Four for suggested improvements to the EIV process.
19. We submit that the definition at (9) for certification by a person overseas needs to be broader than what is proposed. We submit it should be updated to read "by a person in that country who is authorised to undertake certification of documents". This could include, for example, lists of certifiers authorised under other legislation such as those under Australian AML/CFT laws.
20. We should not be comparing to the New Zealand list, as many of the trusted referees on that list are often not comparable with an overseas jurisdiction. Instead, REs should be able to place reliance on a person that is qualified in that country to certify documents. Further, the Supervisors should consider how to address overseas certification requirements from jurisdictions where there is no concept of certification. It may be appropriate, for example, to provide a list of certain professions that REs may rely upon in the absence of clear certification qualifications.
21. We also consider that the list of trusted referees in Part 2, clause 8 should be expanded to include:
  - 21.1. Additional roles that carry legal authority and community trust, such as Māori Land Court officials (Chief Registrars or Regional Manager). This would enhance accessibility, cultural appropriateness, and regional equity while maintaining the same independence and reliability intended in the Code.
  - 21.2. Expanding chartered accountants to also include certified public accountants. There is no clear rationale to accept certification from one professional accountancy body but not another.



### Certification period

22. We support the proposal to increase the certification period from 3 months to 6 months.

### **Proposal four: Electronic identity verification**

23. NZBA supports the inclusion of information from the explanatory note in the IVCOP; having fewer documents to refer to is beneficial.
24. We are also supportive of the proposal to remove the need to verify a customer's name via a second source, which will in our view reduce regulatory burden and make verification simpler for customers.
25. We submit that in limiting reliable and independent sources to DIA and NZTA, New Zealand is not future proofing our methodology, and are limiting the utility of EIV to a domestic use-case. Frequently, REs will have to rely on certification for overseas customers.
26. Considering the proposed changes to certification, it is important that EIV solutions remain suitably flexible. This should include accepting equivalent databases / services in overseas jurisdictions (e.g. the Australian DVS for the Australian passport).

### **Proposal one: Verification pathways**

27. NZBA supports retaining the three existing verification pathways. Our members use all three pathways in different circumstances.
28. Retaining the three verification pathways is consistent with the design intent of the IVCOP, which provides a safe-harbour mechanism for complying with verification requirements under sections 16, 20, 24 and 28 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**).
29. The proposal minimises the potential for any operational disruption, as these pathways accommodate the needs of most customers. This allows reporting entities (**REs**) to design an efficient and flexible programme that meets compliance obligations in a convenient manner, as each existing pathway serves a distinct customer context:
  - 29.1. Part 1 (Documentary verification): The primary mechanism for customers presenting original documents.
  - 29.2. Part 2 (Certified copies): Enables non-face-to-face onboarding and supports customers unable or unwilling to attend in person.
  - 29.3. Part 3 (Electronic verification): Promotes digital efficiency and aligns with evolving identity management practices.



- 30. Removing or narrowing any pathway would undermine the flexibility intended when the Code was promulgated, which is essential for ensuring equitable access and proportionality, particularly for remote, regional or mobility-limited customers.
- 31. As discussed further below, the outcome of Proposal 3 may impact the acceptance of certified copies.
- 32. We also support the introduction of the Digital Identity Services Trust framework as a fourth verification pathway, and consider it will help REs to adopt more efficient digital identity solutions while maintaining strong assurance levels.

## **Proposal two: Documentary identity verification**

### Current identity documents

- 33. NZBA considers that the current list of identity documents is fit for purpose and should be retained.
- 34. These documents provide a good range of options, are well known / understood, and are workable. They have been in place for more than a decade and crucially are familiar to customers, frontline staff and assurance teams.
- 35. While there may be scope for further refinement and additions to Part 1, as noted in paragraphs 37 – 45 below, we consider it is beneficial to keep the current list to help mitigate any unintended consequences of restricting access to banking unnecessarily. Retention avoids unnecessary disruption to customers and retraining for staff of REs. For completeness, we have included comments on further suggested improvements below.
- 36. We are supportive of the proposed minor changes, which should assist with clarity without altering the underlying framework.
- 37. NZBA submits the following refinements would help to strengthen proportionality while remaining consistent with the principles of section 16(1)(a) of the AML/CFT Act (“verify identity through reliable and independent sources”).

### *Minors*

- 38. Opportunities should be explored to increase documents that would typically be accessible for this group, for example student ID cards.
- 39. A birth certificate should be sufficient when linked to a guardian’s identity:
  - 39.1. Under Part 1(2)(a-d) (primary non-photographic ID), a birth certificate is already a valid identification document.





- 39.2. For minors' accounts, requiring additional secondary documents may create unnecessary barriers.
- 39.3. Linking a minor's birth certificate to a parent's or legal guardian's verified identity provides sufficient assurance for low-risk minor accounts.

#### *Additional forms of ID*

- 40. In relation to the Consultation's proposed change to 2(f), we note that the current IVCOP states that "Points 2(e) – (g) above are not an exhaustive list ...". There is a risk that by adding further sources / types of ID, the list becomes more prescriptive and, as a result, REs may take the view that the listed forms of ID are the only acceptable forms. REs value the current flexibility, which supports financial inclusion. It is therefore important to retain this flexibility.
- 41. The updated IVCOP should retain, or strengthen, the clarification that the list is not exhaustive and that REs retain the right to use other documents where appropriate.
- 42. If additional ID types are going to be included, we submit a SuperGold card should be treated as an acceptable secondary or supporting (where the SuperGold card includes a photo) form of identification. This would be of benefit for elderly customers opening a bank account, and would mitigate the need for using exception handling procedures which importantly supports broader financial inclusion initiatives.
- 43. We also submit that valid, government-issued drivers licences should be included as an acceptable secondary or supporting form of photographic identification without the requirement to also hold an international driving permit (**IDP**).
  - 43.1. An IDP does not provide any additional identity verification beyond that of a foreign drivers licence; it exists as an internationally recognised translation of a home country's drivers licence and can be obtained very easily.
  - 43.2. For example, in Australia and New Zealand, all that is required to obtain an IDP is upload a recent (uncertified) photo, scan a licence and pay a credit card fee. It is also not a document people generally hold unless they are travelling.
  - 43.3. Removing the requirement for an IDP would create a better customer experience, and be particularly helpful for obtaining ID for overseas individuals and is unlikely to increase the money laundering or terrorism financing risk.
- 44. Internationally, it is generally permissible to accept any government-issued identification card, not just passports. Adopting this approach would simplify the process in New Zealand.



### *Other minor amendments / clarifications*

45. NZBA also considers the following minor amendments would improve the identity verification process:
- 45.1. Expansion of “bank statement”: We submit the reference to “bank statement” at clause 3 should be expanded to include electronic statements and other bank-issued documents.
  - 45.2. Expired New Zealand passports: The existing guidance on accepting an expired New Zealand passport through the exceptions handling process should be incorporated into the IVCOP.<sup>2</sup>

### Part 1 application to face-to-face verification

46. We consider that the proposed statement set out at Question 4 is already implied by the IVCOP and accompanying legislation. Inclusion of an explicit statement may require REs to update their onboarding solutions to enable this to be captured / recorded, increasing compliance requirements without effecting a change in current practice.

### **Proposal six: High-risk customers**

47. NZBA supports the IVCOP applying to high-risk customers, and note that this is common industry practice currently. Categorising a customer as high-risk or low-risk generally occurs after identity verification requirements have been met. The risk-rating of a customer should not impact identity verification methods.
48. Applying the IVCOP to high-risk customers helps to ensure consistency of baseline verification while allowing enhanced due-diligence requirements (as mandated by s 24 of the AML/CFT Act) to be layered on top. This supports a clear, more predictable compliance framework without reducing safeguards, providing greater certainty to REs.

### **Proposal seven: Beneficial owners and persons acting on behalf**

49. We note that our members have a range of views on this proposal, which we anticipate will be addressed in individual submissions.

### **Proposal eight: Originators of wire transfers**

50. NZBA largely supports the proposal as it is clarifying existing interpretation. Where identity has been previously verified to Code standard, re-verification should not be

---

<sup>2</sup> See [Guidance on Expired Passports as Identification for CDD](#) (2019).



mandated unless reasonable doubts arise (consistent with section 31 of the AML/CFT Act). This avoids unnecessary duplication and aligns with the risk-based approach.

51. However, we consider that certain channels present different risks so that risk-based conditions are appropriate.

51.1. In practice, the majority of wire transfers are now requested via online banking platforms. Access to these platforms is controlled (via authenticated login). Users who have the ability to authorise a wire transfer via this channel, have already been subject to identity verification and we agree it is not necessary to require this again, unless there were reasonable grounds to doubt the adequacy or veracity of the identity verification previously conducted.

52. It would also be beneficial if the IDVCOP could clarify the approach required to be taken in the circumstances where the customer is an Existing Customer as defined under the AML/CFT Act. We submit that the IVCOP should state that the requirement is for customers onboarded since the commencement of the AML/CFT Act only.
53. If full CDD was required for all pre-AML/CFT Act customers before doing a wire transfer, full remediation projects would be required, or wire transfers would need to be checked prior to sending, which does not align with the Government's programme of burdensome compliance reduction, would risk a significant slow down of the payment process as well as being operationally challenging.

### **Proposal nine: Other conditions**

54. We support the expansion of exception handling procedures. However, it is important that the IVCOP maintains flexibility in the approach to exception handling – prescription around how and when to use exception handling procedures needs to be avoided.
55. In order for the proposal to be most effective, it needs to remain risk-based, with REs able to determine when and how they apply it.
56. For example, it may be more appropriate to use the term “any alternate measures”, as usually all possible options would have been exhausted to verify the customer's name and date of birth – therefore rendering “increased or more sophisticated” verification unworkable.