AML / CFT

Anti-money laundering and countering financing of terrorism

Explanatory Note: Electronic Identity Verification Guideline

For Part 3 – Amended Identity Verification Code of Practice 2013

July 2021

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Reserve Bank of New Zealand
Te Pūtea Matua

Te Tari Taiwhenua
Internal Affairs

Introduction

1. This Explanatory Note and guideline should be read in conjunction with the Amended Identity Verification Code of Practice 2013 (**the code**).

2. The code was approved in October 2013. This followed implementation of the Electronic Identity Verification Act 2012 and the Identity Information Confirmation Act 2012.

3. This Explanatory Note and guideline replaces the previous Explanatory Note that was published by the Supervisors in December 2017. It includes additional content identifying commonly used electronic sources in New Zealand. It also sets out the supervisors' expectations when they review or inspect a reporting entity's Electronic Identity Verification (**EIV**) procedures, policies and controls. Various examples of EIV practices are included at the end of this guideline.

4. This guideline has been produced by the supervisors under s132(2) of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act). It cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. This guideline does not constitute legal advice.

What is electronic identity verification under the code

5. EIV is where a customer's identity is verified remotely or non-face-to-face.

6. EIV has two key components, both of which must be satisfied:

   - Confirmation of identity information via an electronic source(s); and
   - Matching the person you are dealing with remotely to the identity that they are claiming (*i.e. are they the same person*)?

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

8. For electronic identity verification, it is important to remember that an 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 received from the person being dealt with online, including audio-visual link or video conferencing technology.
   - An uploaded image of the person's identity document(s).
   - An email, app or internet platform through which the reporting entity receives information or copies of identity documents.
   - The third-party provider (EIV Provider) that a reporting entity uses to conduct its EIV.

Using a single independent source

9. Under the code, a reporting entity can satisfy EIV requirements from a single independent electronic source that is able to verify an individual's identity to a high level of confidence.

10. 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.[1]

11. When using an electronic source that is able to verify an individual's identity to a high level of confidence, you are not required to separately link the individual to the claimed identity.

12. 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. Other biometric possibilities in the future could include iris structure or fingerprint information*.

Using two reliable and independent matching sources

13. The code also allows a reporting entity to verify an individual's identity from at least two electronic sources. The individual's name and date of birth must be verified from one source, whereas only the name must be verified from another source. The two electronic sources must be:

    - Reliable, and
    - Independent, and
    - Match each other.[2]

14. 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.

15. Supervisors expect that the primary electronic source used to verify name and date of birth of an individual that is in New Zealand is:

• Confirmation Service (DIA)	Government source - name and date of birth verification from passport, birth, deaths and citizenship database.
• NZ Driver Licence (NZTA)	Government source - name and date of birth verification from NZTA driving licence records.

[1] At the time of publication, only a verified RealMe® identity can meet this requirement in New Zealand. By biometrically matching the person's photo and identity details against New Zealand government records (the electronic source) it verifies the person's identity to a high level of confidence.

[2] A reporting entity may verify an individual's identity from two or more "reliable and independent" sources via a single third-party EIV provider.

16. Other common electronic sources in New Zealand that could be used as the second source to verify an individual's name include:

    - Credit Bureaus
    - Companies Office
    - Land Registry (LINZ)
    - Vehicle registration (NZTA)

17. Where two matching reliable and independent electronic sources are 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 (whether biometrically or otherwise). None of the electronic sources listed in paragraphs 15 and 16 above incorporate such a mechanism.

Additional methods required to link the customer to their claimed identity

18. 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 clause 18 of the code requires that a reporting entity must adopt **additional methods** that will be used to supplement it, or to otherwise mitigate any deficiencies in the process. The additional methods must ensure that the person that the reporting entity is dealing with is the genuine holder of the identity they are claiming.

19. Some examples of additional methods are noted below.[3] At the end of this guideline are further examples of how a person being dealt with online may be linked to the identity that is being verified. How this can be achieved depends, to some extent, on the type of reporting entity, its products and services and how these are delivered to customers. Other considerations include whether an occasional transaction is being conducted, or whether a business relationship is being established (which may enable alignment with the AML/CFT Act's delayed verification provisions).

    - Require the first credit into the customer's account or facility to be received from an account/facility held at a New Zealand registered bank in the customer's name that cannot be altered or changed. The list of New Zealand registered banks that do not allow the customer to alter or change the payer name is provided in the appendix.

      If you are utilising this as an additional method, it is important that you have controls in place to ensure the name matches your customer's identity. This is because there are no industry standards relating to naming conventions and character restrictions in banking systems can impede the completeness of a person's name received. If the payment arrives and the name does not match, there must be an escalation process.

[3] Note: supervisors do not consider the use of video conferencing technology to engage with a customer as a method to link the customer to the identity they are claiming under the code (see example 5 below).

- 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 (either physically or via an electronic channel) to the reporting entity before the customer's account or facility is fully operational e.g. before any withdrawals/debits can be conducted.

- Robust steps to ensure the authenticity of any identification document electronically provided by the customer. This will require the use of an EIV provider able to confirm the identity document is authentic and that it was issued to the person being dealt with online. This process must ensure the document has not been forged, altered or tampered with in any way, including the photo on the document (see example 2 below).

  If you are using an EIV provider in this way, you should assess and document the level of assurance provided. We expect your EIV provider to be able to assist you with this. Considerations should include how the images are obtained, for example incorporating liveness test, the steps taken to confirm the authenticity of the image on the identity document and the reliability of facial recognition software used.

- 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. For example, phoning a customer on a fixed line through an employer.

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

This is not an exhaustive list and there may be other adequate additional measures. Please contact your AML/CFT Supervisor to discuss further.

Document your EIV procedures

20. Under clause 18 of the code, reporting entities that utilise EIV must clearly document as part of their AML/CFT Programme how all the relevant criteria within the code are satisfied. The key principle is that your EIV procedures are documented. The following information should be described:

Include	Explanation
When you will use EIV.	Will you use it: • As the default method • As a backup • When you can't face-to-face on-board someone • In conjunction with face-to-face • For NZ residents only • For lower risk customers only, etc.
EIV provider and product.	If you rely on a third party to conduct EIV (EIV Provider), detail your EIV provider and the EIV product that you are using. If you are using multiple providers

Include	Explanation
	or different providers for NZ resident customers and those abroad, explain this. You should also explain how you are using the product. Do you log into your provider's product and enter your customers' details directly or is there an integrated feed? Are you using a combination of different offerings from your provider?
The electronic source(s) used to verify the person's name and date of birth.	What selected electronic sources are you verifying your customer's name and date of birth against in NZ and elsewhere? EIV providers often allow you to choose a range of electronic sources to verify customer details against.[4] You must explain which sources your EIV providers are using. You must ensure the sources you choose meet all relevant requirements or provide the necessary level of assurance. It is harder to fake identity information across multiple data sources. The more sources used to verify identity information, the increased assurance this provides.
Record keeping processes.	You should describe how you will capture and record the information submitted by your customer and the evidence of the EIV (the result). Many EIV providers will not keep that information for longer than a few days.
How you check your records that a prospective customer's details have not previously been used.	These are not unique requirements because you use EIV. These are requirements for all customer due diligence (CDD) activity (refer to clauses 5 and 16 of the code).
Exception and escalation processes	Unsuccessful EIV requires escalation and individual review. In some circumstances, a person's identity may not be verifiable to the required level. Rather than accepting a lower standard, it may be necessary to adopt face-to-face or certified copy verification under Part 1 or 2 of the code.

21. Your documented EIV procedures should make it clear if you are using a single independent source to high level of confidence; or two (or more) reliable and independent matching sources.

[4] Note: In our experience, all EIV providers offer multi source verification for customers resident in NZ and Australia. This broadly uses the same databases. For access to EIV sources outside of NZ and Australia, there are different EIV providers depending on the country. We are aware of some offshore based providers promoting EIV solutions that do not verify customer identity information against an underlying source (such as a government database). If you have customers outside of NZ and Australia, you should discuss this with your EIV provider to ensure the EIV sources they offer, meet your requirements.

Single independent source

22. If using a single **independent electronic source** able to verify an individual's identity to a high level of confidence, you should document how this level of assurance is met.

Two reliable and independent sources

23. If using two matching **reliable and independent** electronic sources, you must follow and document the steps set out in clauses 17 and 18 of the code. This should include your consideration of:

Include	Explanation
Clause 17 of the code requires you to assess and document their reliability and independence. This should include your consideration of: a) Accuracy b) Security c) Privacy d) Method of information collection e) If the source can link a customer to their claimed identity f) Whether the information is maintained by a government body or pursuant to legislation g) Whether the information has been additionally verified from another reliable and independent source	If you rely on an EIV Provider, we would generally expect your EIV provider to assist you to assess and document the reliability and independence of the electronic sources they use. You should keep evidence of your analysis. We also expect that you treat an outsourced EIV provider as you would all key outsourced relationships. We may ask you to explain the due diligence (DD) performed on engaging your EIV provider and any ongoing DD performed to ensure the EIV provider continues to meet your expectations. How you continue to assess independence and reliability of your electronic sources should be part of your regular DD review and should be documented as well.
Clause 18 of the code requires that if you are using two electronic sources with no mechanism to link customer to claimed identity, you implement additional methods to link the person you are dealing with online to the identity they are claiming to be (being the identity you are verifying).	You must document what additional methods are used and explain how this supplements your EIV or mitigates any deficiencies in the verification process (see clause 18(c) of the code).

Customers who established a business relationship before 30 June 2013

24. Electronic sources could also be used to verify or 'top up' 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. In some situations, the linking mechanism may not be required for the existing customers if the reporting entity has evidence that the customer was 'linked' via face-to-face when they first established a business relationship.

Examples

Example 1. NZ based reporting entity accepting domestic and overseas customers (Additional method – initial deposit requirements)

ABC Limited, a reporting entity based in New Zealand, has customers in New Zealand and two other countries. To verify a new customer's name and date of birth, ABC Limited:

a) Utilises an EIV provider and two electronic sources in all three countries and always checks the verification result is positive.
b) The electronic sources used by ABC Limited have mechanisms that check that the identity is genuine but do not have mechanisms that link the person being dealt with online to that identity.
c) Requires the customer's first deposit of funds to the reporting entity from a bank account in the customer's name. There are controls in place to ensure this occurs, that the name matches when the bank transfer is received and there is an escalation process if it does not.

Supervisor view:
ABC Limited's EIV process provides a pathway to comply with the code. To ensure compliance, ABC Limited must follow the steps set out in clauses 17 and 18 of the code. This includes assessing whether the electronic sources in the respective countries are maintained by a government database or pursuant to legislation. In practice, the supervisor's view is that the primary electronic source used for name and date of birth verification should be a government database.

As none of their EIV Provider's electronic sources link the person being dealt with to the identity being verified, it is necessary to adopt an additional method. ABC Limited's process for checking the transfer is received from a bank account in customer's name is a way of meeting this requirement. They should also confirm the transfer is from a bank registered in New Zealand and listed in the Appendix to this guideline. If the transfer is from a bank registered in New Zealand but **not** listed in the Appendix to this guideline, they should adopt a separate method for linking the customer to their identity. For overseas customers, a credit from an account at a bank registered in a country with sufficient AML/CFT systems is likely sufficient to link the customer to their identity.

Example 2. Identity document authentication, then verification from two reliable and independent reliable and independent electronic sources (Additional method – robust electronic tamper checks and facial recognition software)

DEF Limited uses an EIV provider with access to electronic sources, including the DIA Confirmation Service. However, neither the DIA Confirmation Service nor any of the other electronic sources that the EIV provider uses incorporate a mechanism to determine whether the customer can be linked to the claimed identity (whether biometrically or otherwise).

Therefore, additional methods are required under clause 18 of the code. The EIV provider offers a solution that can validate the authenticity of an identity document,

as well as use facial recognition software to match the image of the person on that document with an image of the person being dealt with online.

DEF Limited wants to electronically verify the identity of a new customer, who is a New Zealand citizen. To verify the new customer's name and date of birth, the EIV provider:

a) Collects the full name and date of birth of the customer, along with their New Zealand passport number and its expiry date.
b) Captures an image of that passport.
c) Captures an image of the person being dealt with online using a robust liveness detection system.
d) Uses facial recognition software to match the image of the person being dealt with online to the image of that person on the New Zealand passport.
e) Checks are undertaken to assure there has been no tampering with the passport, including validating machine-readable zone data and other passport security features.
f) Verification of the full name and date of birth of the customer, and their NZ passport, is then undertaken using the DIA Confirmation Service.
g) The customer's name is also verified from another electronic source.

Supervisor view:
DEF Limited's EIV process provides a pathway to comply with the code. This combines verification of the name and date of birth of the customer from two reliable and independent sources, together with additional methods to link the person being dealt with online to the identity being verified.

In this example, the additional method occurs at steps (c), (d) and (e) of the process. It occurs when the image of the person being dealt with online is captured and then matched using facial recognition software to the image on the passport, with tampering checks also performed on the passport. The matched identity is then verified from two reliable and independent sources. One of these is the DIA Confirmation Service that verifies the person's identity and passport from the DIA passport database.

Example 3. Facial recognition software technology as a standalone solution without electronic sources

GHI Limited uses an EIV provider with a facial recognition technology solution. Similarly to example 2) above, the EIV provider's product requires a customer to take a photo of their passport, together with an image captured from a live video feed of themselves. Using the EIV provider's facial recognition technology, an image of the customer captured from the live video feed is then matched to the image on the passport. Checks are also undertaken to validate security features on the image of the passport, including for the machine-readable zone. However, there is no verification undertaken to authenticate that the identity on the passport is genuine.

Supervisor view:
This does not comply with the code. Even though a facial recognition software solution is being used, there is no verification from any reliable and independent electronic source.

Example 4. Delayed verification (Additional method – delayed verification in person)

MNOP Limited is often instructed by a new customer by phone or email to establish a business relationship relating to a captured activity. At a later point the customer must attend the office of MNOP Limited in person to sign a contract and other paperwork related to the captured activity. MNOP Limited's EIV process is as follows:

a) Collect identity information from the new customer and ask them to email a scanned (uncertified) copy of their passport information page.
b) Undertake verification of the customer's name and date of birth from two reliable and independent electronic sources, one of which verifies the passport using the DIA Confirmation Service.
c) Commence providing the captured activity to the customer, but not conclude it.
d) When the customer attends the MNOP Limited office, the original passport must be sighted.

Supervisor view:

MNOP Limited's EIV process provides a pathway to comply with the code when establishing a business relationship with a client. The customer's identity is being verified from two reliable and independent electronic sources, but neither source incorporates a method to link the customer to the identity they claim to be. This required additional method is achieved later when the customer attends the office with their original passport. This relies on the delayed verification provisions of s16(3) and s24(3) of the AML/CFT Act but is conditional on:

a) Remote onboarding being essential not to interrupt normal business practice; and
b) Money laundering/terrorism financing risks are effectively managed through procedures of transaction limitations and account monitoring or (if the reporting entity is not a financial institution) through other appropriate risk management procedures; and
c) Verification of identity is completed as soon as practicable once the business relationship has been established.

Note that the delayed verification provisions are only applicable when establishing a business relationship. (i.e. they may not be relied on for a customer that is undertaking an occasional transaction or occasional activity through a reporting entity).

Example 5. Video conferencing technology

QRST Limited onboards all customers remotely. It uses an EIV provider with access to electronic sources, including the DIA Confirmation Service to confirm the identity information. To then link the customers to the identity they claim, QRST Limited will arrange a video conference call with the customer. During the call, they request the customer to hold up the identity document on the photo page.

Supervisor view

QRST Limited's method for remotely matching their customer to the identity that they are claiming **does not meet the requirements of the Code.** A purely visual human eye inspection on a video conference call is insufficient to link the customer to their claimed identity to satisfy the requirements of the code.

Example 6. RealMe
When WXY Limited onboards a new customer, it verifies the customer's name and date of birth from a single independent electronic source using RealMe. This is only for customers that have a verified RealMe identity.

Supervisor view:
This complies with the code. RealMe is enabled by the Electronic Identity Verification Act 2012, the purpose of which is to provide "a high degree of confidence in an individual's identity". There is a biometric matching process in that the person must have their photo taken, which is then matched to the photo in the DIA passport database (or in some circumstances, the Immigration NZ database). This provides "a high degree of confidence in an individual's identity".

High-risk customers

25. The code is only applicable for customers that are assessed by the reporting entity as low to medium risk. It does not apply to customers assessed as high-risk. The code states that increased or more sophisticated measures should be applied for high-risk customers.

26. While the code is not applicable for high-risk customers, the supervisors' view is that it can still be used as a basis for a reporting entity to develop its name and date of birth verification procedures for high-risk persons.

27. However, the supervisors consider that the code should be the minimum level of verification that is applied to a high-risk customer. The types of further verification steps that are required for high-risk customers (beyond those outlined in the code) will depend on the customer and the reason they are assessed as high-risk.

28. If the reporting entity is satisfied that the high-risk customer's name and date of birth are correct, it may not be necessary to adopt any additional verification steps beyond those in the code. Instead, the reporting entity should place increased focus on other components of CDD. This may include obtaining further information on the nature and purpose of the business relationship and/or verifying the customer's source of funds or wealth (as part of enhanced CDD).

29. However, if the reporting entity is not satisfied that the high-risk customer's name and date of birth are correct, then additional verification steps (beyond those in the code) should be adopted. For customers being verified by EIV, these could include:

    - Using three or more electronic sources to verify name and date of birth;
    - Adopting further additional methods, including in combination with each other;
    - Requiring the customer to visit the reporting entity in person with their original identity documents.

New and emerging risks and threats

30. Reporting entities should consider new and emerging risks or threats to the EIV tools and processes that they utilise, including associated mitigation.

About codes of practice

31. Codes of practice are intended to provide a statement of practice to assist reporting entities to comply with certain 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.

32. 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. Note: This guideline does not operate as a 'safe harbour'.

33. 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:

• Identification Management Standards available on the Department of Internal Affairs' website

• Te Kāhui Māngai, a directory of Iwi and Māori organisations available on Te Puni Kokiri website.

Appendix

First credits that can be relied upon to determine whether the customer can be linked to their claimed identity can come from any of the following registered banks:

ANZ Bank New Zealand Ltd

ASB Bank Limited

Australia and New Zealand Banking Group Limited

Bank of Baroda (New Zealand) Limited

Bank of China Limited

Bank of China (New Zealand) Limited

Bank of India (New Zealand) Limited

China Construction Bank Corporation

China Construction Bank (New Zealand) Limited

Citibank N A

Commonwealth Bank of Australia

Heartland Bank Limited

Industrial and Commercial Bank of China (New Zealand) Limited

Industrial and Commercial Bank of China Limited

JPMorgan Chase Bank NA

Kiwibank Limited

Kookmin Bank

MUFG Bank, Ltd

Coöperatieve Rabobank U.A. trading as Rabobank Nederland

Rabobank New Zealand Limited

Southland Building Society

The Co-operative Bank Limited

The Hongkong and Shanghai Banking Corporation Limited

TSB Bank Limited

Westpac Banking Corporation

Westpac New Zealand Limited

Version History

2013	Amended Identity Verification Code of Practice - Explanatory Note 2013
December 2017	Amended Identity Verification Code of Practice - Explanatory Note 2017 - Replaced Explanatory Note 2013 - Updated to include clarification regarding requirement to link person to claimed identity through additional methods.
July 2021	Explanatory Note: Electronic Identity Verification Guideline – 2021 - Replaced Explanatory Note 2017 - Includes additional content regarding documenting EIV procedures, supervisor expectations and examples of EIV solutions.