KitLegal.

Identity Verification Software

Identity verification software is great but it is important to understand it is only one part of the overall customer due diligence process and when working with any verification software provider, you need to understand the components they are covering and what they are not covering to ensure the whole process is mapped out.

We find some firms who use this software forget there are other parts of the process and they get missed.

The initial customer due diligence process involves:

1. If the Customer is an individual, taking reasonable steps to establish the customer is who they claim to be.
2. Collecting KYC information (the info you need to collect is different for an individual vs company vs trust) about the customer, any beneficial owner(s) of the customer, any person on whose behalf the customer is receiving a designated service or any person acting on behalf of the customer (like POA etc).
3. Determining if the customer (or any beneficial owner or agent) is a PEP or designated for targeted financial sanctions.
4. Identifying the customer's ML/TF risk based on the KYC information collected.
5. Determining if you need to apply enhanced CDD.
6. Determining if you can apply simplified CDD or use deemed compliance provisions.
7. Collecting additional KYC information as appropriate to the customer's ML/TF risk, and to mitigate and manage that ML/TF risk.
8. Verifying KYC information (about the customer, beneficial owners, agents etc) using reliable and independent data, that's appropriate to the customer's ML/TF risk.

You can complete some of these steps at the same time.

What you will need to work out is what parts of the process the identity verification software provider is providing and which parts you will still need to undertake.

In particular, you need to understand how they handle complex structures. For instance, if you have a client who is a company, and there are shareholders who are trusts, how is that handled? To comply with the law, you need to go through each structure, and where trusts are involved, you will need to look at the trust deeds to find out who the ultimate beneficial owners/controllers are and then do the KYC process on those individuals. In some complex structures this can have multiple layers of companies and trusts involved.

In our experience, for simple 'mum and dad' investors, identity verification software can work really well. For Australian companies where no trusts are involved, it also works well due to publicly available information. However, because there is no central register of trusts in Australia, there is currently no way to identify a structure where trusts are involved (i.e. where the ASIC search shows that shares are non-beneficially held) without seeing the trust deed and exploring further. These are the things you just need to work through with the provider to be clear on the process and map it out.

You will also need to gather information about source of wealth - there are 2 things to capture here. First, source of funds for a particular transaction and second, source of overall wealth for the customer. Most professional services firms will be meeting obligations around source of funds and source of wealth in information gathering processes and understanding the client's overall circumstances, context and history to be able to give them advice. You need to undertake further enquiries about source of funds or source of wealth and verify source of funds/wealth information only where things don't add up or don't make sense or there is some other risk trigger involved. For instance, if someone has excessive wealth that makes no sense based on what you know about them or you see adverse media about them for instance.

Ongoing customer due diligence obligations apply for business relationships.

Identity verification software and outsourcing

AUSTRAC has released detailed guidance about entering into outsourcing arrangements and engaging an identity verification software provider constitutes an outsourcing arrangement. We provide an AML/CTF Outsourcing Checklist with all of the detailed requirements as part of our product offering (for anyone on the waitlist, just ask us if you need this now).

Record keeping obligations

Under the new AML Rules, AUSTRAC makes it clear you need to keep evidence of what you have done to verify identity but don't have to keep the actual ID doc itself if you can evidence it in another way.

Usually, the easiest way to keep evidence is to keep a copy of what you sighted for verification. However, you can keep a detailed file note specifying that you reviewed an original or reliable copy of trust deed for xyz trust dated [xx] and what information you sighted in the trust deed (i.e. names of trustee(s), settlor, appointor (if there is one), named beneficiaries and for a unit trust, % holdings etc). This can be more work than just keeping a copy! The same with the IDs you reviewed – type of document, date of document, document identifier (i.e. relevant numbers etc) and what information you sighted (full name, DOB and or residential address). As long as your identity verification software provider is providing you with a record of all of this, that's fine.

KitLegal.

Identity Verification Software
November 2025