Key stages in the lifecycle of an ID document in the AML/CTF context

There are a range of obligations under *the Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) where ID documents and ID information may be relevant. This fact sheet steps through some key lifecycle considerations under the *Privacy Act 1988* for the collection, use, disclosure and retention of ID documents and ID information in the AML/CTF context. It also provides answers to several frequently asked questions (FAQs) on this topic.

Read this information in conjunction with the OAIC's privacy guidance for reporting entities under the AML/CTF Act.

Key lifecycle considerations

Privacy by design

The AML/CTF Act does not prescribe a particular method for verification, as how reporting entities verify identity documents to meet obligations depends on the money laundering and terrorist financing (ML/TF) risk. When considering how you handle ID documents and/or ID information to comply with AML/CTF obligations, take a privacy by design approach by considering:

- whether the circumstances surrounding the chosen method of verification are proportionate and justify the privacy risks
- whether less privacy intrusive techniques could be used - escalate to more intrusive information handling only as necessary to meet your AML/CTF obligation (i.e. to address the ML/TF risk)

Depending on the size and complexity of your entity, conducting a Privacy Impact Assessment can help entities design better privacy processes around the handling of ID documents. See the OAIC's Guide to undertaking privacy impact assessments.

Collection

You must limit your collection of personal information (including ID information and ID documents) to what is reasonably necessary to comply with your AML/CTF obligations, and other functions and activities of your entity. Take a data minimisation approach as excessive collection and retention of ID documents is a privacy and security risk.

The AML/CTF Act does not require you to collect, use, disclose or hold copies of full ID documents (including for customer due diligence (CDD), personal due diligence, ongoing monitoring and record keeping).[1]

The amount and nature of personal information that is reasonably necessary to comply with AML/CTF obligations may vary on a case-by-case basis depending on the ML/TF risk. It is your responsibility to be able to justify that a particular collection is reasonably necessary.

A key consideration is whether you could undertake the function or activity, or fulfil your AML/CTF obligations, by collecting less personal information.

For example, instead of requesting a full copy of an ID document via email, could you meet your CDD obligations by sighting the document, only recording relevant fields from the primary ID document or by using digital verification technology which returns a token or Yes/No result?

If you decide to collect a copy of a full ID document because it is merely helpful, convenient or desirable, you will not be able to establish reasonable necessity.

Use and disclosure

You must only use and disclose the ID document or ID details for the purpose you needed to collect it for, such as:

- the specific AML/CTF compliance purpose
- fulfilling other business functions and activities, OR
- for another exception under APP 6 (e.g. if required or authorised under another Australian law).

Retention

If you retain copies of ID documents, set time-limits for each purpose that involves handling of identification information or documents, to help determine if they are still needed, and how long to retain them for.

You must take reasonable steps to destroy or de-identify the ID document copy or ID information when it is no longer needed for your AML/CTF obligations or another permitted purpose under the APPs. Only retain the minimum information that you need. There are exceptions, and you do not need to destroy or de-identify personal information where you are required by or under an Australian law or a court/tribunal order to retain it. See the FAQs below for an example.

You should not rely on s 111 alone (of the AML/CTF Act) to continue to retain a copy of an ID document on a long-term basis, as the AML/CTF Act no longer requires this.

1 The use and disclosure of an ID document is also not 'authorised' by the AML/CTF Act under APP 6 solely because the AML/CTF Act does not prohibit it, nor can an entity collect, use, disclose and hold an ID document because it is convenient for, or incidental to the AML/CTF obligations. A law will only authorise using or disclosing ID documents if it does so by clear and direct language. Where there is discretion as to what and/or how an entity will collect information under a relevant law, only collect only what is reasonably necessary to fulfil that obligation. You should also ensure handling of the information is proportionate to the aim of fulfilling the legal obligation, adopting a data minimisation approach where possible. See meaning of Required or authorised by or under an Australian law or a court/tribunal order' under Chapter B of the APP Guidelines for more information.

Frequently asked questions (FAQs)

What ID information can entities retain for record keeping purposes?

Entities must retain certain AML/CTF records (e.g. s.111 of the AML/CTF Act requires retention of information reasonably necessary to demonstrate compliance with CDD). The AML/CTF Act does not require you to retain a copy of the full ID document to demonstrate compliance for record keeping purposes. Instead, it is generally reasonable to keep records of what you did to identify a customer, key details of the identifying information the customer presented (e.g. licence number), the type of document, the outcome of your verification and analysis, identification or assessment of ML/TF risk.

See section J of the OAIC guidance for more advice.

What if another law or court order requires an entity to retain ID documents?

Entities do not need to destroy or de-identify personal information where they are required by or under an Australian law or a court/tribunal order to retain it. For example, state and territory electronic conveyancing participation rules may require the retention of copies of ID documents (time limits may apply).

When can entities use, disclose or hold ID documents for another non-AML/CTF purpose?

There may be other reasons to use, disclose or retain ID documents outside the AML/CTF Act (for example where required by another legislative obligation or for the purpose of fulfilling other business functions and activities, where the collection was reasonably necessary).

In such cases, the information should only be retained for so long as it is needed to comply with those other permitted purposes or legal obligations.

When can entities use, disclose or hold ID documents/ID information for an AML/CTF compliance purpose?

The AML/CTF Act does not require you to collect, disclose or hold copies of full ID documents. It must be genuinely needed based on the specific circumstances (e.g. ML/TF risk and unsuitable alternative verification methods).

In narrow circumstances where it is reasonably necessary for an entity to collect, use, disclose or hold a copy of a full ID document for AML/CTF compliance, the entity can only hold it until that purpose is discharged (or for another purpose for which the information may be used or disclosed under the APPs).

For example, where an entity reasonably needs to collect a full ID document to verify identity for initial CDD, the entity may be permitted to hold it while verifying identity and recording required details from the ID. The entity should not rely on s 111 alone (of the AML/CTF Act) to continue to retain a copy of an ID document on a long-term basis, as the AML/CTF Act no longer requires this.

This fact sheet does not constitute legal advice. An entity may wish to seek independent legal advice where appropriate, for example as to whether another law requires retention of identity documents.