First AML

Australian Standard Operating Procedure

Introduction and Overview

First AML assists reporting entities with collecting and processing KYC/AML documents. This guide shares our methodology for conducting KYC/AML.

Our methodology has been developed in accordance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules) and AUSTRAC customer due diligence reference guides. We regularly update this guide in line with changes in regulations or evolving best practices.

In this guide, "Reporting Entity" refers to you as a client of First AML and "Customer" refers to the individual or entity on whom we are conducting customer due diligence.

Our guide outlines how we collect and process information on your behalf, as First AML is a specialised KYC service provider operating as an agent under section 37 of the AML/CTF Act.

The Reporting Entity is ultimately responsible for approving whether KYC performed by First AML on a Customer is sufficient for meeting your internal compliance programme. In accordance with Part 7 of the AML/CTF Act, the Reporting Entity is required to maintain its compliance programme.

Click to see a visual flowchart of our standard operating procedure

Revision History

Version	Date	Author	Description
0.1	1 June 2021	Hamish Scarborough	Initial documentation
0.2	30 June 2021	Jessie Mao	Documentation update
0.3	31 March 2022	Jessie Mao	Public-facing markups and reformatting
0.4	26 May 2022	Angus Hook	Exceptions register and biometric EIV on new branding
0.5	24 April 2023	Jessie Mao	Documentation update Biometric Update

1.0 Levels of Customer Due Diligence

First AML conducts Customer Due Diligence in line with the Act, as follows:

1. Simplified due diligence
2. Standard due diligence
3. Enhanced due diligence

Below are the criteria for what falls into each level, and how First AML conducts checks for each level.

1.1 Simplified Due Diligence

1.1a Criteria

First AML will conduct Simplified Due Diligence when the customer is:

- a company that is either:

1. a domestic listed public company;
2. a majority-owned (50%+) subsidiary of a domestic listed public company; or
3. licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company.

- trust that is either:

1. a managed investment scheme registered by the Australian Securities and Investments Commission (ASIC);
2. an unregistered managed investment scheme that only has wholesale clients and does not make small-scale offerings;
3. registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or
4. a government superannuation fund established under legislation.

1.1b What do we collect?

Where the entity is a simplified company, First AML will obtain one of the following documents:

1. a search of the relevant domestic stock exchange;
2. a public document issued by the relevant company;
3. a search of the relevant ASIC database;

4. a search of the licence or other records of the relevant regulator.

Where the entity is a simplified trust, First AML will obtain one of the following documents:

1. a search of the relevant ATO, ARPA, and ASIC databases;
2. a search of the licence or other records of the relevant regulator;
3. confirmation of the Trust's regulated/licensed status from the customer.

In conducting Simplified Due Diligence, First AML will also collect the following additional information:

1. Full legal name(s) of the simplified entity
2. Registered address
3. One of the following where applicable:
    a. Australian Company Number
    b. Australian Business Number
    c. Stock Symbol (Ticker)
    d. Registered scheme/licence number

Please see Parts 4.3 and 4.4 of the AML/CTF Rules for more information about Simplified Due Diligence verification procedures for companies and trusts.

1.1c What do we verify?

Here is an example that helps to explain what we collect for Simplified Due Diligence:

Self-Managed Superannuation Fund

In the case of a Self-Managed Superannuation Fund, we will collect the following information:

1. Superannuation Fund Name
2. Australian Business Number
3. Full Name of the Trustee/Principal Members

We will verify the following information:

1. Superannuation Fund through the Australian Taxation Office (ATO) SuperFund Lookup
    a. Where this is not able to be verified, we will ask for a certified copy of the Fund Trust Deed and apply Standard Due Diligence procedures.

1.2 Standard Due Diligence

1.2a Criteria

Standard Due Diligence is conducted when the customer is (but is not limited to):

1. an individual
2. a domestic or registered foreign company operating in a country that is deemed a low or medium risk or a cooperative jurisdiction by the Financial Action Task Force (FATF)
3. an unregulated Trust e.g. Family or Unit Trust

1.2b What do we collect?

First AML collects the following information on the customer for Standard Due Diligence:

1. the person's full legal registered name(s);
2. the person's date of birth;
3. the person's residential address;
4. the person's address or registered office, and
5. the company identifier or registration number.

1.2c What do we verify?

Here are some examples that help to explain what we collect for Standard Due Diligence for the most common types of entities:

Company

In the case of a Company, we will collect the following information:

1. ASIC or a certified copy of a foreign equivalent e.g. certificate of incorporation, register of members.
    a. If this can not be obtained, First AML will request for a disclosure letter written by a company legal counsel or a similar individual with effective control over the entity.
1. Full legal names and date of birth for all beneficial owner(s) (e.g. directors and any shareholders with 25% or more shareholding interest).

We will then verify the following information:

1. ASIC or a certified copy of a foreign equivalent e.g. certificate of incorporation, register of members.
2. All Beneficial owners with 25% or more shareholding.
    a. In the absence of any shareholders that meet the threshold, First AML will verify one individual with effective control over the entity or transaction e.g. superior voting rights, veto rights, authorised signatories etc.

For overseas entities, First AML will seek to obtain the relevant company records.

In the absence of a beneficial owner with 25% or more shareholding whether directly or indirectly, First AML will verify at least one individual with superior control, voting rights, direct day-to-day supervision etc.

Trust

In the case of a Trust, we will collect the following information:

1. Certified copy of the Trust Deed and any amendments
    a. If this can not be obtained, First AML will request a disclosure letter outlining the Trust details.
2. Full Name of the Trust Deed, Trustee(s), Settlor, Appointor(s), Protector(s), Guardian(s), and any named beneficiaries

We will then verify the following information:

1. Certified copy of the Trust Deed and any amendments
2. All Trustee(s), Appointor(s), Protector(s), and Guardian(s) as per the 'Individual' or 'Company' verification procedures outlined in Part 4.2 of the AML/CTF Rules.
3. If applicable:
    a. Non-discretionary beneficiaries
    b. Settlor(s) when the amount settled is over $10,000
4. If this is a Unit Trust, we will verify all unitholders who hold 25% or more of the total units.
5. If the beneficial owner(s) of the Trust are companies or individuals, we will proceed based on the verification standards of an individual or a company.

For any other legal entity types, First AML will collect and verify relevant documentation in line with procedures from Chapter 4 of the AML/CTF Rules.

1.3 Enhanced Due Diligence

1.3a Criteria

First AML will only conduct Enhanced Due Diligence if instructed by the Reporting Entity to do so (e.g. because the customer is deemed high-risk). Please ensure that the risk level and the CDD level are appropriately filled out in the 'AML Profile' section.

Please note that a Reporting Entity **must** apply enhanced customer due diligence in the following high-risk situations (but not limited to):

1. When the risk level for money laundering/terrorism is determined to be high e.g. customer operates in a country/region that is:
    a. deemed a high-risk or non-cooperative jurisdiction by the Financial Action Task Force (FATF)
    b. prescribed foreign countries

c. subject to sanctions
d. known tax havens
e. known to provide support to terrorist organisations; or

2. Where the customer or the beneficial owner(s) of the customer is a foreign (PEP) politically exposed person.

Please refer to Parts 15.8 to 15.11 of the AML/CTF Rules for further guidance.

1.3b What do we verify?

In addition to the Standard Due Diligence verification, First AML may collect (if agreed upon with the Reporting Entity) information to verify the source of funds/wealth of the customer. The source of wealth/funds evidence will be collected for the direct customer.

By default, the source of wealth evidence will be collected for the customer unless otherwise instructed by the reporting entity within the First AML Notes field.If the reporting entity deems that the source of wealth and/or source of funds information is insufficient, they can 'Rework' the case to ask for more information to be collected.

1.4 Ongoing Due Diligence

There are two ways for a Reporting Entity to request Ongoing Customer Due Diligence (**OCDD**) cases. These cases must be a previously verified entity within the Reporting Entity's own First AML database.

1. "Re-verification required" - First AML will re-verify the entity to ensure the documentation is up to date and there have been no changes to the entity structure. These cases will be charged 50% of your complex fee.
2. "No verification required" - The case will immediately move to the 'Ready to Review' section on the Platform and will not be checked by Specialists. There is no charge for this type of case request.

For individual cases, First AML will send out a new Electronic Verification Form (EIV Form) and will re-verify their details to ensure it is up to date. This will be charged at the standard individual fee.

2.0 Electronic Identity Verification

First AML verifies the identity of individuals by collecting an individual's full name, date of birth and address and verifying their full name and either their date of birth or residential address electronically.

Reporting entities can configure on or off the following:

- Collection of identity documents e.g. Australian Passport, New Zealand Drivers Licence.
- Anti-tampering to ensure the identity document's validity and to check for any fraud measures.
- Biometric to ensure the individual is a legitimate live individual and whether they match the photo on their identity document.

For a full list of data sources used for electronic identity verification, as well as PEP/sanctions/adverse media checks, please reach out to your Customer Success Manager or First AML Support at support@firstaml.com

These documents are verified against the relevant electronic databases. Individuals are sent the First AML verification form and asked to supply images of both of the identity documents requested.

First AML will seek explicit consent from the end-user before conducting any electronic verification, excluding screening checks.

Consent is provided through our user-friendly verification forms. If a client has not completed verification through our forms, our Specialists will go back and explicitly ask for their consent. Consent may be collected verbally over the phone (recorded) or via text or email.

How we meet Safe Harbour

For medium or low-risk individuals, First AML will use 'safe harbour' procedures to verify the individual's identity. First AML will electronically verify the person's name and either the individual's date of birth or residential address against at least two reliable and independent electronic sources.

If electronic verification can not be achieved, First AML will contact the customer to provide certified documents. Please see the Documental Certification Standards below.

3.0 Documental Certification

When First AML can not electronically verify an individual, First AML will revert to acquiring certified copies of identification and a non-certified copy of a proof of address document.

It is preferred that the documentation has been certified by a Trusted Referee within 24 months of the case request date. Passports will be accepted up to 24 months past their expiry date.

3.1 Approved Certifiers

- Lawyers
- Chartered Accountants
- Justice of the Peace/Notary Public
- Sworn Member of the Police
- Registered Medical Doctor
- Registered Teacher
- Minister of Religion
- A person who has the legal authority to take statutory declarations or the equivalent in your state/territory

3.2 Certification Wording

First AML will request to the customer that the certification must have the following information

> *"I, [Trusted Referee Name], hereby certify that this is a true and correct copy of the original document which I have sighted, and it represents a true likeness of this individual."*

- Date of certification
- Signature of Trusted Referee
- Profession of Trusted Referee
- Registration Number if applicable

4.0 Case Processing Procedure

4.1 Opening Cases

To open a new case, the reporting entity ("you") must request a case in the First AML Platform and provide:

- the name of the customer,
- customer type (Trust, Company etc.)
- the name and contact details of at least one contact person. This contact person must not be an internal staff member, i.e. Author or Agent unless it is essential.

Any case received by 4.30 pm Australian Eastern time will be assigned to a First AML Specialist and opened on the same day. Cases received during the weekend or after 4.30 pm Australian Eastern time will be opened on the next business day.

If a case is requested and any relevant documentation is held, such as certified Trust Deeds or Partnership agreements, please use the documents tab to upload these before submitting them.

Please do not upload any ID documents into the documents tab, as this will delay the verification process of your clients. Uploading ID documents may not include the essential elements of electronic ID verification. These include photographs of the front and back of the ID document, residential address confirmation, and consent to electronically verify. All of these elements are captured in the form our Specialist team sends to your clients.

4.2 Urgent Cases

If there are urgent cases, please try to submit the case as soon as possible to give the First AML team a reasonable amount of time to process the case. First AML cannot guarantee that the case will be completed by the deadline.

If the case is urgent, please notify our Specialist team by noting this in our Platform via the Compliance Team Notes with a date the case needs to be completed.

4.3 Awaiting information from customers

First AML will request information from customers being verified and process information as soon as practicable after it is received. Any delay to case processing is generally due to non-cooperation or slow response from a customer being verified.

4.4 Keeping track of case progress

Reporting Entities can monitor the progress of cases in the First AML Platform. Verification results for individuals who have been verified will be shown, and documents received can be reviewed.

Any pertinent information will be contained in the 'notes' section, otherwise, the Reporting Entity can assume that First AML is awaiting information from the customer if the case is still in progress. Our Specialist team will do everything they can within reason to get the KYC case completed. The Reporting Entity should assume that this is happening behind the scenes. Not every detail of every action will be noted as it is designated to be a summary.

Reporting entities will be able to see all contact made from the First AML Specialist team in the 'Activity' tab. The Activity tab within the First AML platform will have all emails, phone calls, and text messages summarised by the First AML Specialist.

Please refer to the First AML platform before contacting First AML to discuss a case.

4.5 Reminders

First AML will send periodic reminders to customers who are not cooperating or are slow to respond. Reminders may be in the form of

- Text messages
- E-mails
- Phone calls

After each reminder is sent, it will be logged in the 'Activity' tab. First AML is not liable for any further reminders or follow-ups to individuals who are non cooperating with the process.

4.6 Email templates

First AML uses email templates when contacting customers to obtain information. The Reporting Entity name and relevant case information are inserted into the template, but the template cannot otherwise be modified. Please refer to Appendix A for the email templates.

First AML will CC (copy in email) one person from your organisation to our initial CDD/KYC request emails. This may be a generic inbox. If one is not chosen, this will default to the case requester. The purpose of this is to add a layer of familiarity and ensure your clients are comfortable that First AML has been instructed as your CDD/KYC provider.

4.7 Use of the 'notes' section

First AML will use the 'notes' section to record any pertinent information regarding the case. Reminders and information we are waiting on will be detailed under the 'Activity' tab.

If First AML uncovers an anomaly during the case processing, this will be documented in the 'notes' field and should be reviewed before approving the case. Anything of note e.g. Positive PEP Check will be reported to the Compliance Officer before ready for review.

4.8 Dormant case policy

If there has been no response or noncooperation from a customer for 14 days then First AML will mark the case as 'Dormant'. The Reporting Entity will not be notified, and the case will be invoiced at the end of the month it was marked Dormant.

If a case has been put 'On Hold' for more than 14 days, the case will be moved to 'Dormant.'

The charge for the Dormant case will be the standard case fee.

4.9 Abandoned case policy

To abandon a case, please notify the Specialist team via the Compliance Team Notes section. If a case is abandoned after a follow-up has been done, there will be an abandoned case fee. The charge for abandoned cases will be the per-case fee.

4.10 Exceptions Policy

Any exceptions to our usual verification and identification procedures for individuals or entities can be requested within each case. Compliance Officers, Platform Admins and First AML Specialists/Admins can request exceptions by using the "Add exception" tool within an individual or entity's profile. By doing so, First AML can acknowledge any exceptions that a reporting entity would like to make to its compliance programme.

Users can choose between Permanent and Temporary exceptions. Permanent exceptions will remain in place for all existing and future client cases. Temporary exceptions can be granted in the temporary absence of materials to complete necessary identification or verification. These temporary exceptions will be labelled "Unresolved" while waiting for further action from the end-user, and "Resolved" once the exception is no longer required.

4.11 Retrieval / Consent Process

As part of all new case requests, First AML will complete a database scan before opening the case and contacting the main case contact with an information request. This scan covers our whole ecosystem. Where there is existing valid information within the database, we will seek consent to reuse all possible relevant information and confirm if there have been any changes to the beneficial ownership structure. Any outstanding information required will be requested.

Due to privacy reasons, if there is a close match (but not an exact match), First AML will not start with a retrieval request. We will instead ask the customer to confirm if they have previously been verified by First AML and to confirm the entity/individual's name.

4.12 Case Approval Process

First AML will complete the CDD/KYC process per our Standard Operating Procedure (this document) and the AML/CTF legislation. Note that the legislation does have some room for interpretation, and so judgement will be applied on a case-by-case basis. The ultimate approval of a case will be dependent on your compliance programme, risk assessment, and any other internal controls that may be in place.

With this in mind, once a case is completed by First AML, it will be placed in the Ready for Review section of the platform. From this point, the elected Case Approver will receive an email to review the case is Ready for Review.

Appendix A - Email Templates

Email to Client Contact

Dear %Name%,

First AML has partnered with %Customer Name% to conduct CDD/KYC for %Case Name%.

The next step is to collect some additional information from you.

Please provide the following

- [Relevant AML requirements for individuals and entities within the case]

Submit information

Verification made easy

Check out our helpful guide for troubleshooting tips and answers to your verification FAQs. If you need additional help, please create a support ticket to get in touch.

Thank you,
First AML
support@firstaml.com