First AML

United Kingdom

Standard Operating Procedure

First AML

Contents

Introduction and Overview 3
Revision History 4
1.0 Customer due diligence 5
1.1 Standard customer due diligence (CDD) 5
1.1.1 Standard CDD: Process and collection 5
1.1.2 Standard CDD: Information collection for Entities 6
1.1.3 Standard CDD: Acting on behalf 8
1.2 Simplified customer due diligence (CDD) 8
1.2.1 Simplified CDD: Information collection 9
1.3 Enhanced customer due diligence (CDD) 9
1.3.1 Enhanced CDD: Criteria 10
1.3.2 PEPs: Identification of politically exposed persons (PEPs), their relatives or close associates 10
1.3.3 Sanctions 10
1.3.4 Enhanced CDD Collection 11
1.3.5 Enhanced CDD Collection: Manual Source of Funds 11
1.3.6 Enhanced CDD Collection: Manual Source of Wealth 12
1.4 Ongoing Due Diligence/Reverification 12
1.5 Recordkeeping 13
1.6 Screening 13
1.6.1 Screening check 13
1.6.2 Screening Profile 14
1.6.3 Screening result review 14
1.6.4 Screening result escalation 15
1.7 Ongoing Monitoring 15
2.0 Verification Procedure: Individuals 16
2.1 Electronic Identity Verification (EIV) 16
2.1.1 EIV Components 16
2.1.1 EIV Verification levels 17
2.1.2 EIV Verification Levels: KYC Only (Failed Result) 18
2.2 Manual Verification 18
2.2.1 Manual verification: Approved document certifiers 19
2.2.2 Manual verification: Certification wording 19
2.2.3 Manual verification: Customers unable to produce standard documentation 19
3.0 Verification Procedures: Common Entity Types 20
3.1 Private limited companies 20
3.2 Overseas companies 21
3.3 Publicly listed entities 21

3.4 Partnerships, Limited Partnerships (LP), Limited Liability Partnerships (LLP) 21
3.5 Trusts 22
3.5.1 Trusts: Corporate trustees 23
3.5.2 Trusts: Beneficiaries 23
3.5.3 Trusts: Pension Schemes 23
4.0 Case Processing Procedures 24
4.1 Opening cases 24
4.2 Urgent cases 24
4.3 Awaiting information from customers 24
4.4 Keeping track of case progress 25
4.5 Reminders 25
4.6 Email templates 25
4.7 Use of the 'Notes' section 26
4.8 Dormant case status 26
4.9 Abandoning a case 26
4.10 Exceptions 26
4.11 Case approval process 27
4.12 Languages/Documents not in English 27
Appendix A: Default Email and SMS Communication Templates 28
1. Secure web form email: Request for documentation – Entities or Individuals 28
B. EIV Email: Request to individual to complete EIV form 29
C. SMS: Request to individual to complete EIV form 30

First AML

Introduction and Overview

This document outlines how First AML UK Limited (**First AML**) conducts customer due diligence (**CDD**) as an agent/outsourced service provider on behalf of its clients (each a **Relevant Person**) in accordance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).

This document is focused on First AML's due diligence service and operating procedure, and outlines how our delivery team interacts with its **Client** and their **Customers**. It is not intended to provide a holistic view of all the necessary information required to be included in a Relevant Person's AML policies, controls and procedures (as required under the MLRs), which remain the sole responsibility of your organisation.

Unless we agree otherwise in writing, First AML's process will not deviate from what is outlined in this document.

The policies and procedures in this document have been developed with reference to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended), the Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Fraud Act 2010 (together, the **Regulations**). In addition, best practice steps have been taken from the following industry guidance (together, the **Guidance**):

- Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)
- Legal Sector Affinity Group (LSAG) Anti-money laundering guidance for the legal sector - 2021
- The Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector – Part I 2020
- Anti-Money Laundering Guidance for the Accountancy Sector - 2021
- Estate agency business guidance for money laundering supervision - 2021
- Amended Money Laundering and Terrorist Financing Regulations (MLRs) 2022
- Economic Crime (Transparency and Enforcement) Act 2022

First AML acts as an agent of the Relevant Person and does not assume responsibility for compliance under these regulations.

First AML

Revision History

Version	Date	Author	Description
0.1	22 April 2025	Jessie Mao	Initial documentation
0.2	29 September 2025	Ella May Lorelei Neilsen Kate Green	Major update and revision: document restructured, new sections added, language aligned further with UK terminology and content rewritten for clarity.

First AML

1.0 Customer due diligence

As per the requirements of the Regulations, the result of the Relevant Person's risk assessment should dictate the level and extent of due diligence undertaken on the Customer.
First AML will not conduct or review the risk assessment on behalf of any Relevant Person.
Relevant persons should ensure to instruct First AML of the level of CDD required for each Customer within the 'AML Profile' section. Please see a link to our help centre article here.

First AML will proceed with the performance of CDD based on the due diligence level instructed by the Relevant Person.

First AML can perform Standard, Enhanced, or Simplified CDD. The data that is required to be collected and reviewed will depend on whether First AML is conducting Standard, Enhanced, or Simplified CDD.

1.1 Standard customer due diligence (CDD)

By default, a Relevant Person will be required to conduct Standard CDD. In these situations, a Relevant Person must:

a) identify the customer unless the identity of that customer is known to, and has been verified;
b) verify the customer's identity unless the customer's identity has already been verified; and
c) assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

A customer's identity for CDD consists of several aspects, including the customer's name, current and past addresses, date and place of birth, physical appearance and, if applicable, their financial circumstances.

The identity of a customer who is not a private individual consists of a combination of its constitution, its business, its legal form, and its ownership and control structure.

1.1.1 Standard CDD: Process and collection

First AML will conduct Standard CDD upon instruction by a Relevant Person. Standard CDD procedures will be conducted in line with the Regulations and Guidance.

The customer type can be any of the following (but is not limited to):

- Natural person(s);
- Private limited companies and unlisted companies (the UK and overseas);
- Trusts and similar legal arrangements such as foundations and charities;

- Partnerships, including limited partnerships and UK limited liability partnerships, limited liability companies, incorporations; and
- Societies, places of worship, schools, clubs and associations.

The customer type will determine what information First AML collects through the due diligence process.

The overall CDD measures that must be carried out involve:

a) identifying the customer, and verifying their identity;
b) identifying the beneficial owners (where relevant), and verifying their identities; and
c) identifying, assessing and, where appropriate, obtaining information about the purpose and intended nature of the business relationship or transaction.

1.1.2 Standard CDD: Information collection for Entities

First AML collects the following information to verify a Customer, all beneficial owner(s) of the Customer (which includes ultimate beneficial owners of non-natural customers), and those purporting to act on behalf of the Customer:

Natural person(s):

- The customer's full legal name(s);
- The customer's date of birth;
- The customer's address; and
- relationship to the customer (if not the customer).

Legal entities (i.e. private limited companies):

- Corporate name;
- Company/registration number;
- Country of incorporation;
- Registered address;
- Details of directors (full name, year and month of birth and country of residence/nationality);
- Details of any other person with significant control (full name, year and month of birth and country of residence/nationality);
- Details of beneficial owners and intermediate companies at more than 25%;

A beneficial owner of a body corporate, other than a listed company, as meaning any individual who:

- exercises ultimate control over the management of the body corporate; or

- ultimately owns or controls, directly or indirectly, including through bearer shareholdings or other means, more than 25% of the shares, profits or voting rights in the body corporate; or otherwise controls the body corporate.

First AML will collect the following:

- Proof of registration for the company either by downloading an excerpt from the relevant local company register or via the customer. This may include one or more of the following:
    - Details from the relevant company registry, confirming details of the company and the director/s and their addresses e.g. UK Companies House Company Snapshot and Confirmation Statement/Annual Returns; or
    - Information from a reputable electronic verification service provider,
- Details of current company officers (i.e. directors and company secretary) and shareholders.
- Confirmation from the customer whether the company has any nominee directors, nominee shareholders, general partners or shares held in bearer form.
    - What this means is that no one is nominated outside of what is seen in the provided company documentation to hold shares or control over the entity on behalf of someone else. This is just a Yes or No answer.
    - Please note this is not collected if the entity is a company limited by guarantee with no share capital.

If the company ownership cannot be ascertained by publicly available documentation and the ownership structure is complex, First AML may request the following:

- Certified Shareholding Structure Chart
    - This must include all ultimate beneficial owners holding over 25% of the company we are verifying. If there are no beneficial owners holding over 25% this must be indicated on the chart.
    - We require the structure chart to be certified by a General Counsel, Lawyer, Chartered Accountant or regulated entity.
    - This individual must be independent to the entity and cannot be a director, member or shareholder.
    - The certification date of the Chart must be within 6 months of the case opening date.

For overseas entities we may collect different documentation depending on the jurisdiction.

- US Entities
    - For Limited Liability Companies we will collect an Operating Agreement and Register of Members/Owners

    - For Corporations we will collect a Register of Directors and a Shareholding Register

- British Virgin Islands & Cayman Islands
    - We may collect a Certificate of Incumbency, Register of Directors and Register of Members

For all entities that have over two directors/officers/trustees/board members, First AML will request a nomination from the case contact(s) to verify two individuals who have more day-to-day involvement or control over the transaction and/or entity.

1.1.3 Standard CDD: Acting on behalf

Where a person (the intermediary, agent or representative) purports to act on behalf of the Customer, First AML will:

- verify that the intermediary, agent or representative is authorised to act on your customer's behalf (i.e. obtain written confirmation from your customer, power of attorney documents, etc);
- identify and verify the intermediary, agent or representative of the customer; and
- verify the identity of the intermediary, agent or representative via EID&V or certified documents.
- if there is a power of attorney involved we will collect a copy of the power of attorney or lasting power of attorney document and verify their identity

1.2 Simplified customer due diligence (CDD)

In certain lower-risk situations, Simplified CDD may be applied to entities. First AML may conduct Simplified CDD if the Customer is not based in a high-risk jurisdiction and is:

- a public administrator or a publicly owned enterprise;
- an individual resident in a geographic area of lower risk (as decided by the Relevant Person);
- a credit or financial institution which is subject to supervision requirements in national legislation e.g. FCA registered entities;
- implementing the 6th Directive and supervised for compliance with those requirements in accordance with the 6th Directive e.g. regulated professional service;
- a company listed on a regulated market (including majority-owned subsidiaries) and the location of the regulated market; and any majority (50%+1) or wholly-owned subsidiaries of such companies. This includes when a company is majority-owned by multiple parties that are publicly listed.

Please refer to this link for HM Treasury's list of high-risk jurisdictions. Please note this should not be a blanket application, and that the Relevant Person should still consider conducting Simplified CDD on a case-by-case basis.

First AML will also conduct Simplified CDD when instructed to do so by the Relevant Person.

Relevant persons should instruct the level of CDD required for the customer within the 'AML Profile' section. Please refer to our help centre article here.

Simplified CDD procedures will be conducted in line with the requirements of the Regulations and Guidance.

Many customers, by their nature or through what is already known about them by the Relevant Person, carry a lower risk of money laundering or terrorist financing. Where a Relevant Person has determined that a customer presents a low risk of money laundering, based on appropriate, documented evidence, Simplified CDD measures may be applied.

Where a Relevant Person applies Simplified customer diligence measures, it must:

a) continue to comply with the Standard CDD measures but may adjust the extent, timing or type of measures undertaken to reflect Simplified CDD determination; and
b) carry out sufficient monitoring of any business relationship or transaction which are subject to those measures to enable it to detect any unusual or suspicious transactions.

First AML will not determine the level of due diligence required where not in line with the regulations as above but will rely upon the Relevant Person identifying and instructing First AML as to the level of due diligence required for each customer.

1.2.1 Simplified CDD: Information collection

For Simplified due diligence, we will collect the following information:

- Customer full legal name;
- Customer registration numbers;
- Regulatory status (if applicable);
- Listing status (if applicable);
- Registered office address and if the different, principal place of business; and
- Evidence confirming the customer's regulatory or listing status from an official independent third-party source.

1.3 Enhanced customer due diligence (CDD)

Where higher risks are identified, Relevant Persons are required to undertake Enhanced CDD, and in respect of customers with whom they have a business relationship, Enhanced monitoring, to manage and mitigate the risks. Potentially higher risk situations may be influenced by:

a) customer risk factors, e.g. some types of company formation can be a higher risk due to the ability to conceal beneficial ownership;
b) country or geographic risk factors, the Regulations contain a high-risk country list and all countries present on the list must be subject to Enhanced CDD; and

c) product, service, transaction, or delivery channel risk factors e.g., where the Relevant Person has not met a customer face to face this can heighten the risk.

Where a customer is assessed as carrying a higher risk, then depending on the circumstances (for example, particular features of the transaction), it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from.

Categories that have been specifically identified under the Regulations as requiring Enhanced CDD include:

a) any business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties is established in a high-risk third country;
b) where the relevant person has determined that a customer or potential customer, is a Politically Exposed Person (**PEP**), or a family member or known close associate of a PEP;
c) any case where the Relevant Person discovers that a customer has provided false or stolen identification documentation, and the Relevant Person proposes to continue to deal with that customer;
d) any case where a transaction is complex or unusually large; and
e) any case identified as one where there is a high risk of money laundering or terrorist financing, either by the Relevant Person or in information made available to the Relevant Person by the authorities.

Where the risks of money laundering or terrorist financing are higher, Relevant Persons must conduct Enhanced CDD measures consistent with the risks identified.

Examples of other Enhanced CDD measures that, depending on the requirements of the case, could be applied for higher-risk business relationships include:

a) obtaining and, where appropriate, verifying additional information about the customer and any beneficial owner;
b) obtaining information on the source of funds or source of wealth of the customer;
c) obtaining the approval of senior management to undertake the transaction, and
d) requiring settlement to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

1.3.1 Enhanced CDD: Criteria

First AML will conduct Enhanced CDD when instructed to do so by the Relevant Person.

Relevant Persons should instruct the level of CDD required for the customer within the 'AML Profile' section. Please refer to our help centre article here. Enhanced CDD procedures will be conducted in line with the requirements of the Regulations and Guidance.

1.3.2 PEPs: Identification of politically exposed persons (PEPs), their relatives or close associates

A PEP is an individual or a relative/close associate of an individual who has been entrusted within the last year with prominent public functions by a public institution, an international body, or a state, including the UK, excluding any middle-ranking or more junior official.

Please refer to the FCA guidance: FG17/6: The treatment of politically exposed persons for anti-money laundering purposes for further information regarding engaging with PEPs as customers.

If a positive match is identified in our Screening Report (see Section 1.6.4: Screening result escalation), we will flag this to your compliance team for escalation. No further work (e.g. follow-ups) will be conducted until the compliance team instructs First AML to proceed with the next steps.

1.3.3 Sanctions

All customers and associated parties will be screened against relevant international sanctions lists, including those issued by the UK, UN, EU, and US (OFAC), as appropriate and based on the screening profile selected by the Relevant Person within our platform.

If a potential sanctions match is identified in our Screening Report (see Section 1.6.4: Screening result escalation), First AML will flag this to your compliance team for escalation. No further work, including follow-up actions, will be undertaken until the compliance team provides instructions to proceed.

It remains the responsibility of the Relevant Person to confirm whether a true match exists and to ensure compliance with applicable sanctions obligations, including obtaining any required licences or authorisations.

1.3.4 Enhanced CDD Collection

In addition to the Standard CDD information collected, First AML may collect Source of Wealth or Source of Funds of the natural person(s) or of the body corporate(s).

Please note the Relevant Person must collect any additional information on the intended nature of the business relationship. First AML will not collect certified copies of Source of Wealth evidence.

Our team will include the First AML Source of Wealth/Source of Funds guidelines sheet with any SoW or SoF request, outlining the below requirements specifically for your customer.

1.3.5 Enhanced CDD Collection: Manual Source of Funds

When a **transaction amount is provided within the AML profile and the CDD Level is Enhanced**, First AML will proceed to collect Source of Funds information and supporting documentation from the Relevant Person(s).

The documentation collected will differ depending on the source of the funds to be used in the transaction. This will total the transaction amount noted on the case.

We also ensure that the below documentation is supported by a written statement from the customer which confirms the Source of Funds for the individual or entity.

We may collect, but are not limited to, the following:

- Salary - 3 x payslips & 3 x months of corresponding Bank Statements for the account the salary is deposited into
- ISA Savings - 3 x months of ISA bank statements and 3 x months of corresponding Bank Statements showing transfers into the ISA account
- Property Sale - Completion Statement (or Memorandum of Sale, if the sale has not yet completed) and corresponding Bank Statement showing the sale funds being received
- Inheritance - Copy of the Probate or equivalent documentation confirming entitlement to the estate and corresponding Bank Statement showing funds being received
- Mortgage - Mortgage Agreement / Decision in Principle, or email confirmation from the mortgage broker confirming the amount the customer will be borrowing
- Gift - Declaration of Gift Form completed by the giftor, confirming their contact details, the monetary value of the gift

We will also collect the corresponding documentation to the above provided, this may include three months bank statements showing income received or bank statements showing funds from source deposited.

First AML will not accept screenshots of bank accounts, investment accounts or any other relevant evidence. We also ensure the documentation provided includes the account holder's name.

1.3.6 Enhanced CDD Collection: Manual Source of Wealth

First AML will conduct **Source of Wealth** checks when the **CDD Level within the AML profile in the platform is noted as Enhanced, and no transaction value is present.**

We will request one of the following from the customer via the platform; dependent on the availability of information and the willingness of the customer to provide financial information and statements.

Option 1 - Documental evidence accompanied by a written statement

- Documentation confirming how the individual/entity has acquired its wealth, examples include:
    - Signed copy of latest financial statements, Loan agreement from Financial institution
    - Bank statements (from last 3 months) showing regular income
    - Investment statements showing income generated from investments
    - Evidence of settlement proceeds, gift or inheritance
    - Copy of Sale and Purchase Agreement of previous property
- Written statement 2-3 sentences long explaining how the documentary evidence provided confirms the Source of Wealth.

Option 2 - Written statement from the customer's solicitor or accountant

- The statement must be a detailed explanation (at least 2-3 sentences long) on how the entity has acquired its funds or wealth. The statement must include the following;
    - The letterhead of the solicitor or accountant (or include the Firm's branding if in e-mail format)
    - Explanation of the relationship and how long the solicitor or accountant has acted for the entity
    - Detailed explanation as to how the entity has acquired its funds or wealth. This must include e.g. purchase price and property address of rental property, information about the employer if funds are derived from salary etc.
    - The statement must be signed and dated by the solicitor or accountant

1.4 Ongoing Due Diligence/Reverification

There are two ways for the Relevant Person to request Ongoing Customer Due Diligence (**OCDD**) cases. These cases must be a previously verified entity within the Relevant Person'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 Analysts. There is no charge for this type of case request.

For individual cases, First AML will check the previous verification that was conducted and if the ID document originally provided is valid, the individual's information will be re-verified. Upon re-verifying the details, there are two aspects which prevent the checks from being completed at this step:

1. Name, date of birth or address fails during the re-verification
2. ID document originally provided is now expired

If either of the above aspects are present during re-verification of the individual, 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 and collect a valid ID document where applicable. This will be charged at the standard individual fee.

1.5 Recordkeeping

First AML will keep records of all AML information within our First AML platform. We will retain your customer information:

1. For as long as necessary to achieve the purposes for which it was collected; or
2. In some cases, where we have an ongoing legitimate need to do so (for example, to comply with legal, tax or accounting obligations, or to resolve disputes), for longer than is necessary to achieve the purpose for which it was obtained.

When First AML no longer has an ongoing legitimate need to process your customer's information, we will either delete or anonymise it. If deletion or anonymisation is not immediately possible (for example, because the information has been stored in backup archives), we will securely store the information and isolate it from any further processing until deletion or anonymisation is possible.

For further information, please refer to the legal page on our website.

1.6 Screening

1.6.1 Screening check

First AML will conduct the following checks as part of our individual verification process - specifically within the individual's Screening Report:

1. PEP check
2. Sanctions
3. Fitness & probity
4. Warnings
5. Adverse media

These checks are run on all individuals designated for individual verification, regardless of if the overall verification is being conducted manually or electronically. The screening element of an individual verification does not require the individual's consent. For more information on individual verifications please refer to Section 2: Individual Verification.

We also run the following Screening checks on all entities verified within a case:

1. Sanctions
2. Fitness & probity
3. Warnings
4. Adverse media

1.6.2 Screening Profile

The customer is able to tailor three elements of their Screening checks in line with their specific needs: Screening Profile, Fuzziness and for Transform customers only, the ability to switch Adverse Media off. This can be configured for you by the First AML team at an overall and First AML 'office'-specific level.

All First AML customers start on the default Standard profile and a "fuzziness" of 30%,. For more information on tailoring your screening checks please see this Help Centre article.

1.6.3 Screening result review

First AML will review any results which arise from a screening check and provide a screening match status to each singular result in the screening report for your review during case approval.

This status is not a final decision made on your behalf, but a tool to assist your team with case review while also ensuring ongoing monitoring is switched off for clear false positive names.

The match status will be determined using the information available using the below criteria. Matches may be confirmed by comparing legal name, date of birth, citizenship, residency, photographs and other available information within the result, as well as supplementary internet searches where needed to confirm.

The following will be recorded against all singular screening hits in a screening report:

"No Match" (green tick)

Will be recorded where the party identified in the screening check is distinctly a false positive match with the individual or entity the check was run against.

"Match" (red flag)

Will be recorded where the party identified in the screening check does appear to be a true match to the individual or entity the check was run against.

"Possible Match" (yellow flag)

Will be recorded by the Specialist if they are unable to fully discount it as a false match, potentially due to limited available information.

At case review, in the event that there are any Match or Possible Match results to observe within an individual's screening report, the case approver will be alerted to this with a red or yellow flag next to the individual's name in the case.

Such statuses are provided for informational and support purposes only and do not constitute a definitive conclusion or regulatory determination. In accordance with the Regulations, the responsibility for assessing, interpreting, and making any final decision in respect of a customer's screening outcome rests exclusively with the Relevant Person.

1.6.4 Screening result escalation

Our team will escalate all positive PEP, Sanctions, Warnings, or Fitness & Probity matches to your compliance team. No further work (e.g., follow-ups) will be conducted until your compliance team instructs First AML to proceed with the next steps.

Positive Adverse Media matches will generally be escalated to your team unless our team determines that the media is irrelevant and does not indicate a credible AML-related risk. In practice, this means we may exclude:

- **Irrelevant information:** media or articles that are not adverse and do not relate to money laundering, terrorist financing, or any predicate offence, or otherwise have no bearing on AML-related risk.
- **Incidental references:** mentions of your customer that are not about their conduct, such as being quoted as a source, providing expert opinion, or appearing in an article for context without implication of wrongdoing.
- **Non-financial or minor offences:** issues that have no connection to money laundering or predicate offences, such as traffic infringements, minor civil penalties, or other low-level matters.

These results will still be recorded in the Screening Report in line with the above process, for your team to review during case approval.

1.7 Ongoing Monitoring

If appropriate for your business type and requirements, First AML offers daily monitoring/rescreening of all individuals and entities following their initial screening in a case. This can be switched on and off by the First AML team. This service falls outside of First AML's service for conducting due diligence, however the platform functionality allows our clients to manage this themselves within the Profiles section of the platform.

Alerts for any changes to an individual's report will be sent to the assigned users (as set by the First AML team in settings) by email to review and note match statuses using the above flags.

Helpful articles:
Ongoing monitoring
Managing ongoing monitoring (for admins)

First AML

2.0 Verification Procedure: Individuals

First AML's individual verification approach focuses on flexible electronic individual verification (EIV) settings set by our clients in line with their own needs. This applies to individuals being verified in their own capacity as a natural person or as part of a wider entity structure.

These settings for individual verification (called *Verification levels*) can be aligned to your internal policies, regulatory obligations, and risk appetite. They are configured by the First AML team who will be happy to discuss any changes you may like to make. Any combination of *Verification levels* can be made available for your case requesters to select when submitting a case - either overall or configured further by First AML 'Office'.

Separately to the default individual *Verification level* set for the case, the case requester must still indicate the relevant transaction's CDD level in the AML Profile tab when submitting. Verification levels only pertain to electronic verification whereas the CDD level notes the overall CDD approach in line with the Regulations. The CDD level does not affect the Verification level for individuals and vice versa.

2.1 Electronic Identity Verification (EIV)

First AML will verify individuals in line with the *Verification level* assigned by the case requester during case submission. Each *Verification level* is made up of a compounding combination of the four following components.

2.1.1 EIV Components

1. **Screening** check: Running the individual's name through various publicly available sources to identify if they are politically exposed, sanctioned, on international warnings lists or fitness & probity lists, as well as if they are mentioned in any adverse media found within reputable sources online. All screening lists can be found in First AML's data sources sheet (lists checked are based on Screening Profile configured in settings).

   +

2. **KYC** check: Verification of the individual's personal details (name, date of birth and residential address) as supplied within the EIV form, each against one independent data source. No customer contact required where used without following components.

   Data sources may include credit bureaus, telco records, government databases and more. *All KYC data sources can be found on First AML's data sources sheet*.

   +

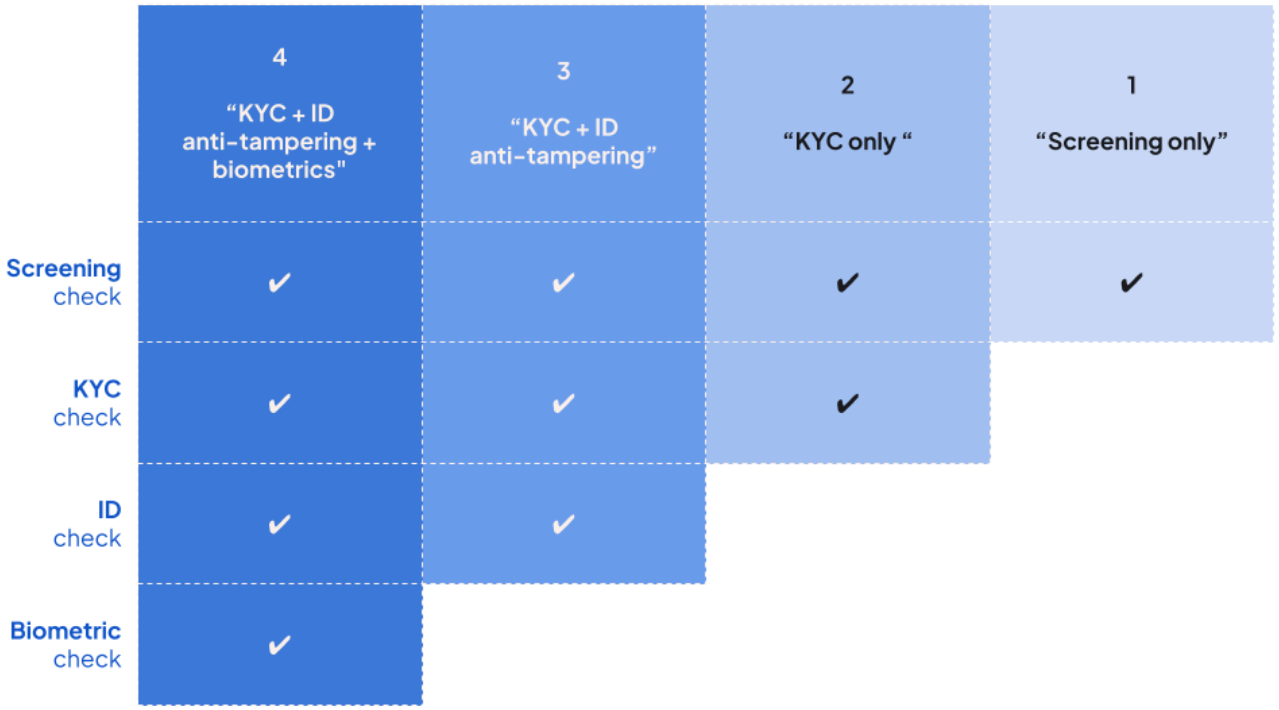
3. **ID** anti-tampering check: Anti-tampering and forgery analysis of the identification supplied. *See Help Centre for more information on the potential results*:

   +

4. **Biometric** check: Verification to biometrically match the individual who completes the EIV form to the ID they have supplied.

   This process involves the use of video to capture liveness and confirm facial recognition checks, and also checks the video itself for legitimacy. *See further information in our Help Centre.*

2.1.1 EIV *Verification levels*



To configure your *Verification level* options, speak to your Customer Success Manager or email support@firstaml.com

Once configured, select desired *Verification level* at case submission:

- Select 'Create new case'
- Select the primary entity type
- Select your verification type (click the downwards triangle to prompt the dropdown*)
- Enter the case name and submit your case

Please note that when you create a case with a specific *Verification level* you cannot change this once the case has been created. If you would like to change the *Verification level* you will need to create a new case and email support@firstaml.com to abandon the current one.

First AML requires explicit consent from the Customer before conducting any electronic verification, excluding screening checks. Consent is provided through First AML's web-based EIV form. If the Relevant person has selected a "KYC only" check, First AML will assume the consent is implied. If a Customer has not completed verification through the EIV form for a full check, First AML will go directly to the Customer and explicitly ask for their consent. Consent can also be provided via the Relevant Person and noted accordingly in the notes in the First AML platform.

2.1.2 EIV Verification Levels: KYC Only (Failed Result)

In some instances for KYC only checks (name, date of birth, address) the individual's details may fail verification. In these instances the AML Specialist assigned to the case will email the case contact with the following:

Hi [Case Requester],

> *Unfortunately the following individual [Add Individual] [Name, Date of Birth and Address] has failed electronic verification through the KYC Only Verification Configuration check.*
>
> *Could you please advise how you would like us to proceed in this instance.*
>
> *Please see the following options:*
>
> - *We request a [Certified copy of their ID and Proof of Address] directly from your client.*
> - *[We request a Secondary ID document to confirm their Date of Birth directly from your client]*
> - *We move the case to Ready for Review, [Client] take a risk based approach and proceed with the case based on your assessment of the risk presented and information at hand.*
>
> *Please note if you require us to collect information from your client directly and their contact information is not yet provided, please provide an email address and phone number for the individual. Further to this, please advise the client First AML will be getting in touch for this information if you have not already done so.*

It is at your discretion to then determine how you would like to proceed in these instances.

2.2 Manual Verification

In instances where First AML cannot electronically verify an individual's details within the platform, initially an external verification system will be utilised, which uses additional data sources to run the individual's details against.

In the instances where an individual's details cannot be externally verified, First AML will revert to acquiring certified copies of identification and/or a non-certified copy of a proof of address document.

Depending on the aspect which fails electronic verification, we will collect the following;

- Name - a secondary ID document will be collected
- Date of birth - a secondary ID document will be collected
- Name & date of birth - a Certified ID document will be collected
- Date of birth & address / name & address - a Certified ID document will be collected
- Address - a proof of address document will be collected, dated within the last three months

When collecting Certified ID from the customer, the document should be certified by a professional person or an individual 'of good standing'. The certification must be dated within 3 months of the case request date. The documents themselves must be valid and current.

To do this, First AML will obtain a certified copy of either:

- one government-issued document which verifies either name and address **or** name and date of birth and with a photograph of the customer; or
- a government-issued document that verifies the customer's full name and date of birth and another supporting document which verifies their name and their address.

2.2.1 Manual verification: Approved document certifiers

- Lawyer / Practicing Solicitor
- Chartered Accountant
- Notary Public
- Justice of the Peace / Magistrate
- Commissioner for Oaths
- Legal Executive
- Licensed Conveyancer
- Authorised Advocate
- Authorised Litigator

First AML will also seek to verify the certifier via reliable online sources to confirm their position.

2.2.2 Manual verification: Certification wording

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

'I, [Certifier 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 (must be within the past three months)
- Signature of Certifier
- Profession of Certifier
- Registration Number if applicable

If the certification wording is not exact but is not materially different it will be accepted. Please refer to our manual verification guidelines for further information.

If the electronic verification form has been completed, the individual's details have failed and subsequently a Certified ID is requested, the 'true likeness' portion of the certification wording will not be required. This is due to the biometric element of the verification already having been completed.

The Certifier also must not be involved in the transaction or business requiring the certification unless they are the appointed general/legal counsel.

2.2.3 Manual verification: Customers unable to produce standard documentation

For individuals who do not hold valid photo ID First AML will collect two certified forms of non-photographic ID. This could include:

- Birth certificate
- Benefits entitlement letter (including government issued pensions)
- HMRC tax notification letter (must be within the last 12 months)

For elderly, vulnerable or disadvantaged customers, First AML will seek to verify these individuals manually.

In most instances, First AML will collect a letter from an appropriate person who knows the individual and can verify the customer's identity as well as any relevant supporting document. Some examples of verification procedures are detailed below.

Customers that are elderly and/or mentally incapacitated:

- Letter from the care home manager confirming identity and residence;
- Letter from a General Medical Practitioner;
- Copies of their expired government ID;
- or Post Office PASS Card; or
- Copies of court documents confirming the individual's identity.

Minor (with government ID)

- Copy of the passport
- proof of address document
- if no proof of address document we collect one from a parent or guardian and verify their identity

Minor (without government ID):

- or Post Office PASS Card; or
- a birth certificate and confirmation of their parent's address or confirmation of address from the register of the school or higher education institution.

Customers with no current permanent address:

- Letter from a householder named on a current council tax bill or a hostel manager, confirming temporary residence; or
- Confirmation via the electoral register.

In these circumstances we may reach out to you to confirm how you would like to proceed depending on your compliance program.

3.0 Verification Procedures: Common Entity Types

3.1 Private limited companies

Please see Section 1.1.2: Standard CDD: Information Collection for Entities for further details.

3.2 Overseas companies

First AML will endeavour to collect copies of all the above documents where possible. For complex structures, First AML may request a copy of a certified structure chart to ascertain beneficial ownership and control structures.

3.3 Publicly listed entities

We will collect the following information:

- Company full legal name;
- Company number or other registration numbers;
- Stock ticker symbol;
- Registered office address and if different, principal place of business; and
- Evidence confirming the company's publicly listed status. This may include:
    - Dated pages of the website of the relevant stock exchange showing the listing;
    - Articles of the listing in a reputable online third party source; or
    - Information from a reputable electronic verification service provider or online registry.

- If this is a subsidiary, evidence of the parent/subsidiary relationship will be obtained. This may include:

    - The subsidiary's last filed annual returns/confirmation;
    - A note in the parent's or subsidiary's last audited accounts or annual report;
    - Information from a reputable electronic verification service provider or online registry; or
    - Information from the parent company's published reports, for example, from their website.

3.4 Partnerships, Limited Partnerships (LP), Limited Liability Partnerships (LLP)

For partnerships, First AML will obtain the following information:

- Name of the partnership;
- Registration number (if applicable);

- Registered address and the trading address (if applicable);
- Nature of the business; and either;
- Copy of the partnership agreement/deed or any equivalent documents. This should include
    - A list of all partners with beneficial ownership
        - LP: General Partners & any Limited Partner with >25% ownership
        - LLP: Partners with > 25% ownership
    - A list of each partner's voting rights/stake or ownership percentage

First AML will verify the following beneficial owners:

- any individual ultimately entitled to or who controls, (whether directly or indirectly), more than 25% of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; and
- any individual who otherwise exercises control over the management of the partnership.

For Limited Partnerships and Limited Liability Partnerships, First AML will obtain a copy of the limited partnership agreement or any equivalent document. The identity of the general partner will be verified along with any limited partners holding more than 25% beneficial ownership or controlling interest.

If the Partnership deed, capital schedule or other documentation cannot be provided by the customer, First AML may request the following:

- Certified Shareholding Structure Chart, or
- Written statement from a General Counsel, Solicitor or Chartered Accountant dated within the last six months, confirming the ownership breakdown of the entity and if any of the Limited Partners / Designated Members hold over 25% ownership.

3.5 Trusts

Regulation 5 define the beneficial owner for a Trust or any similar legal arrangement, as each of

- The Settlor;
- The Trustees;
- The beneficiaries, or where the individuals benefiting from the Trust have not been determined, the class of persons in whose main interest the Trust is set up, or operates; and
- Any individual who has control over the Trust. e.g. Protector, Appointor, Guardian.

First AML will request an uncertified copy of the Trust Deed and any amendment deed(s) to understand the beneficial ownership and control structure for the Trust.

First AML will analyse the Trust Deed and determine all beneficial owner(s) that need to be verified. Identity verification requests will be sent to them.

If the beneficial owner(s) are individuals or body corporates, we will proceed based on the verifications standards of an individual or a body corporate.

If copies of the Trust documents are unable to be provided, we will ask that equivalent documents from the lawyer, accountant, or Trust services firm involved with the transaction to confirm the below Trust details:

- Full name of the Trust;
- Date of creation for the Trust;
- Country of establishment;
- Registered address of the Trust e.g. where is the Trust currently resident/administered
- Nature, purpose and objects of the Trust (e.g. discretionary, testamentary, bare); and
- Full legal name(s) of the following:
    - Settlor;
    - Trustee;
    - Protector;
    - Guardian;
    - Appointor;
    - Beneficiaries.
- Class of the Beneficiaries (if applicable) e.g. future grandchildren of [X].

The above details will also be noted under the entity notes section of the Trust.

3.5.1 Trusts: Corporate trustees

First AML will request that the director(s) of a corporate trustee company e.g. professional Trust service provider, law firm, accountant, are verified as per Standard CDD requirements. If the entity is regulated we will conduct Simplified due diligence and no directors will be verified. We will attach relevant documentation to confirm this.

When there are more than four directors, First AML will verify two individuals with control, voting rights, direct day-to-day supervision etc. over the entity.

3.5.2 Trusts: Beneficiaries

First AML will note all beneficiaries and potential beneficiaries named in the Trust Deed and any associated documents in the entity notes section.

Where the individuals benefiting from the Trust have not been determined, the class of the beneficiaries will be noted. These individuals will not be verified.

Where the individuals benefiting from the Trust have been determined e.g. payment will be made to them or if they will exercise their vested rights in the Trust for the transaction, First AML will verify these individuals upon request. This should be noted within the 'Compliance Team Notes' section. First AML will, by default, identify and verify any non-discretionary beneficiaries holding over 25% of a Trust.

3.5.3 Trusts: Pension Schemes

For Trust-based Pension schemes, First AML will collect the Trust deed & amendments of the pension scheme, similarly to when verifying a Trust.

For contract-based Pension schemes, First AML will collect the documentation confirming the pension scheme's setup. This is on both an individual level (confirming the contract between the member(s) and the pension provider) and on an overall level, confirming the pension scheme the provider is offering. The latter is often accessible directly from the pension provider's website.

First AML will verify the Member(s) of the pension scheme, in addition to the pension provider, and any other controlling entities/individuals within the Pension scheme.

First AML

4.0 Case Processing Procedures

4.1 Opening cases

New CDD cases must be requested via the First AML platform. When submitting a new case, the case requester will be asked to provide the name of the Customer, customer type (individual, trust, private company etc) and 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 GMT will be opened on the same day. Cases received during the weekend or after 4:30 pm GMT will be opened on the next business day.

Cases submitted with a note, or documents uploaded, will have automatic requests and followup automations switched off to allow for Specialist oversight first. These automations assist with closing your case faster, therefore please only leave a note or upload a document if it is relevant to the case.

Useful documents include:

- Trust Deeds
- Partnership agreements
- Shareholding information or structure charts
- Other company information that will assist with the verification

Please do not upload ID documents you hold on file as we are only able to fully electronically verify those which are supplied directly from your customervia our EIV form. Automatic follow ups can be halted by a note being left in the Compliance Notes in the case.

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 your deadline.

If your case is urgent, please notify us by noting this in the First AML platform via the case *reference*. Or alternatively, please notify us by emailing support@firstaml.com. We will do our best to expedite opening the case, but please note that the same followup schedule will apply for external requests. Urgent cases will be expedited where possible however these cases are still reliant on your customer completing the process quickly.

Please do not indicate this in the Compliance Team Notes as this will inhibit the automated forms from sending.

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

Users 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 'First AML Notes' section, otherwise, you can assume that First AML is awaiting information from the customer if the case is still in progress. We will do everything within reason to get the CDD case completed. You should assume that this is happening behind the scenes. Not every detail of every action will be noted as it is designed to be a summary.

When entities (where applicable) have been completed within the 'Entity' tab, First AML will mark these as green within the structure. Likewise, when an individual's verification is completed, they will be marked as completed under the 'Individuals' tab.

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

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

4.5 Reminders

First AML will send periodic reminders (every 2-3 business days) to customers who are not cooperating or are slow to respond. Reminders may be in the form of:

- Text messages (max 2)
- Emails
- Phone calls

First AML will also send specific follow-up reminders to the customer and case requester, dependent on the day.

- Day 10 - If the customer has been unresponsive thus far, First AML will reach out to the customer manually via email to follow up and prompt them to provide the required information.
- Day 14 - If the customer remains to be unresponsive, First AML will reach out to the case requester, asking them to follow up with the customer themselves.

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-cooperative with the process.

4.6 Email templates

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

First AML will cc one person from your organisation on our initial CDD 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 customers are comfortable that First AML has been instructed as your CDD provider.

The introduction section of your email template can be customised to include relevant information you would like to include in all communications. This can be amended by the First AML Customer Success team.

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 Team before ready for review.

4.8 Dormant case status

If there has been no response or non-cooperation from a customer for 30 business days then First AML will mark the case as 'Dormant'. The case requester will be notified via email when this has happened 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 per case fee.

If you would like us to continue work on this verification we require you submit a new case using the OCDD feature.

When creating the case whilst entering the company name you will see a drop down which you can click. This will bring over any of the relevant information from the previous case. This will also mean automated follow ups restart and you will receive an update on the case on day 14.

4.9 Abandoning a case

To abandon a case, please notify us 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 units-based.

4.10 Exceptions

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 against an individual or entity within a case. By doing so, First AML can acknowledge any exceptions that the Client would like to make in line with its compliance program and action within the case in order to complete the case.

First AML may also reach out to the case requester or compliance team if situations arise that are outside the usual verification process to confirm how they would like to proceed. These situations may include but are not limited to; identity verification, corporate structures, beneficial ownership or Source of Funds.

It is at the discretion of the Relevant Person to determine how to proceed. All correspondence regarding decisions made will be noted and attached to the case.

Platform users can choose between Permanent and Temporary exceptions. Permanent exceptions will remain in place for all existing and future cases for the specific customer. 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 customer, and "Resolved" once the exception is no longer required.

4.11 Case approval process

All cases are peer reviewed by First AML before being sent for review. This may cause a slight delay from when First AML receives the information and when the case is sent for review. We will complete the CDD process in accordance with our Standard Operating Procedure (this document) and the Regulations, however the Regulations do require some interpretation and judgement, which will be applied on a case-by-case basis.

For this reason, the ultimate approval of a case will be by you and dependent on your compliance programme, risk assessment, and any other internal controls you may have 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 First AML platform. From this point, the elected Case Approver will receive an email to review the case.

4.12 Languages/Documents not in English

Where documents are in a foreign language, First AML may ask the customer to provide a translated version where possible (unless the First AML team has a sufficient level of understanding of the language).

First AML

Appendix A: Default Communication Templates

Our team is able to send three types of request from within your case, either to send our EIV form for individual verification or to send our secure web form for general documentation and information collection. Please see the default templates for these here to understand what your customer will receive. Additionally, we may also communicate with your customer via adhoc email where necessary.

1. **Email: Secure web form** - Document or information request (for entities or individuals)
2. **Email: EIV form** - Individual verification request
3. **SMS: EIV form** - Individual verification request

1. Secure web form email template

Subject: **Compliance information request for [Case Name]**

Hello [Name],

Default wording below however this section can be tailored by First AML team in settings:

[Client] has partnered with First AML to conduct CDD/KYC for [Case Name].

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

Please provide the following

- [Information to provide to First AML]

Button:

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

First AML

[Client Name] Case Ref: [Case Reference]
Client ID: FAMLID- [XXXXXXXX]
First AML Case Ref: [First AML Case Number]

Things to note

• This message is sent from an email that does not accept responses, please do not reply.

• We're asking you to do this so [Client] can comply with their obligations under relevant anti-money laundering legislation.

• For information about our data handling and security, please see our Privacy Policy.

2. EIV Form email template

Subject: **[Client] - Identity verification request for [Individual]**

Hello [Name],

Default wording below however this section can be tailored by First AML team in settings:

[Client] has partnered with First AML to conduct Customer Due Diligence / Know Your Customer reviews on [Individual].

We're asking you to do this so [Client] can comply with their obligations under relevant anti-money laundering legislation.

The next step is to verify your identity.

Button:
Verify [Name]'s ID

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

First AML

[Client Name] Case Ref: [Case Reference]
Client ID: FAMLID- [XXXXXXXX]
First AML Case Ref: [First AML Case Number]

Things to note

• This message is sent from an email that does not accept responses, please do not reply.

• We're asking you to do this so [Client] can comply with their obligations under relevant anti-money laundering legislation.

• You can verify your identity using your smartphone or a desktop computer with a webcam. Microphone and camera access for websites must be allowed. Please check your device settings before opening the form.

• Have your passport or Driver Licence ready before opening the form.

• For information about our data handling and security, please see our Privacy Policy.

3. SMS: EIV Form template

"[Client] is required to obtain ID information from you. To verify your identity go to [URL]"