CUSTOMER DUE DILIGENCE OUTSOURCING TO FIRST AML

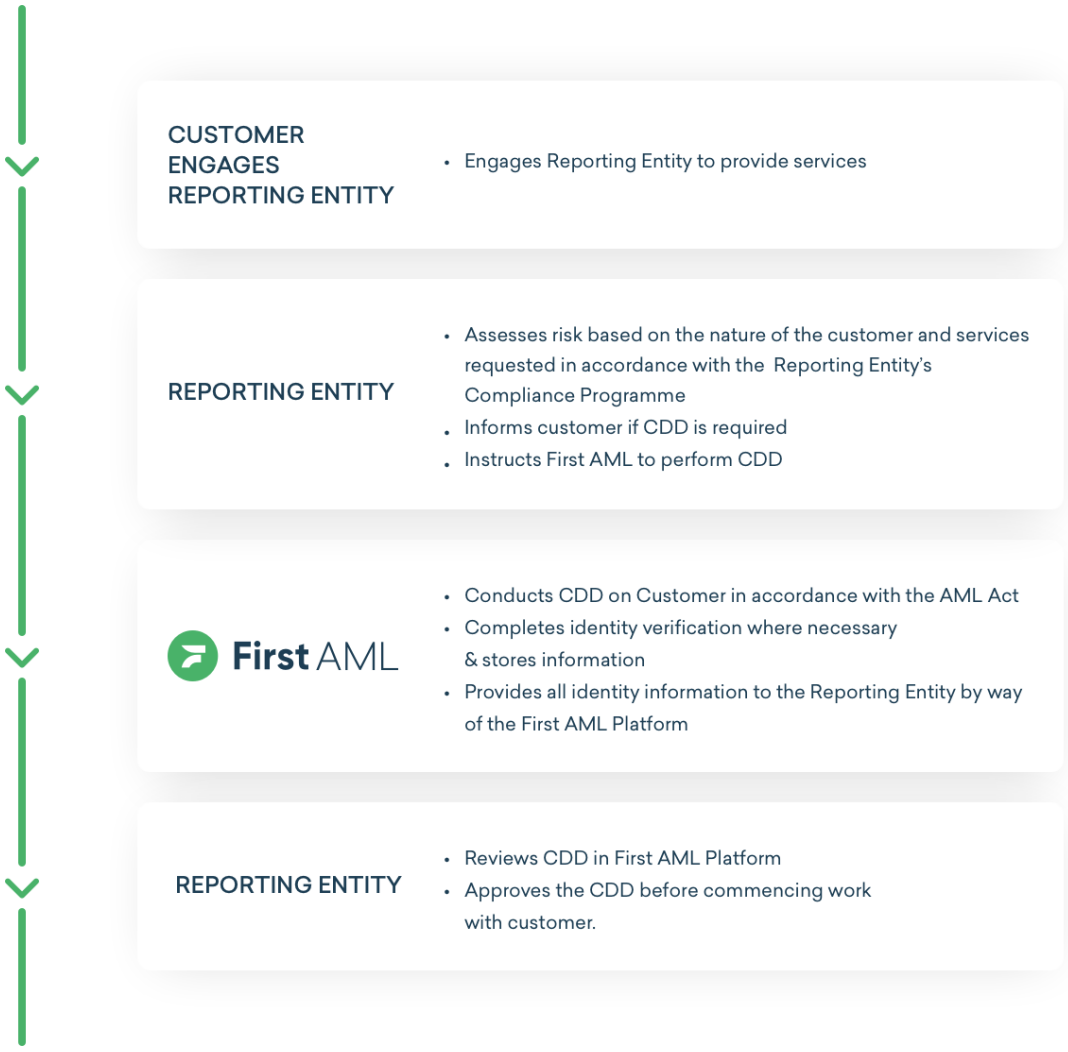
1 Introduction and Overview

1.1 First AML is a specialised customer Due Diligence (CDD) service provider operating as an Agent in accordance with R39 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (amended) (**Regulation**).

1.2 First AML conducts CDD on behalf of a Reporting Entity, liaising directly with its customers to perform the necessary verifications under the Regulation (refer to Figure 1 for an overview). First AML will conduct CDD in line with First AML's Standard Operating Procedure.

1.3 This document outlines how CDD is managed when outsourcing to First AML and sets out the responsibilities of the Reporting Entity and First AML. It does not provide all necessary information required to be included in the Reporting Entity's Compliance Programme or policies in respect of its compliance with the Regulation.

Figure 1: Overview of CDD Process



2 When CDD measures will be applied

2.1 As per R27, the Reporting Entity will apply CDD measures to a customer whenever:

(a)establishes a business relationship;
(b)carries out an occasional transaction that amounts to a transfer of funds within the meaning of Article 3.9 of the funds transfer regulation exceeding 1,000 euros;
(c)suspects money laundering or terrorist financing; or
(d)doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

2.2 As per R28, The Reporting Entity will obtain information about the nature and purpose of the proposed business relationship.

2.3 CDD identification and verification procedures will be applied before the establishment of a business relationship or before carrying out an occasional transaction or occasional activity if the services required are deemed by the Reporting Entity to be a transaction requiring CDD (as defined in the Regulation).

2.4 This regulation applies when a relevant person is required to take any measures under Regulations 27, 28 or 29.

(2) Subject to paragraph (3) or (4), a relevant person must comply with the requirement to verify the identity of the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer before the establishment of a business relationship or the carrying out of the transaction.

(3) Provided that the verification is completed as soon as practicable after contact is first established, the verification of the customer, any person purporting to act on behalf of the customer and the customer's beneficial owner, may be completed during the establishment of a business relationship if—

(a)this is necessary not to interrupt the normal conduct of business; and
(b)there is little risk of money laundering and terrorist financing.

(4) The verification by a credit institution or a financial institution of the identity of a customer opening an account, any person purporting to act on behalf of the customer and any beneficial owner of the customer, may take place after the account has been opened provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed.

3 Capture

3.1 The Reporting Entity is responsible and liable for determining if the services required by the customer are transactions that require CDD.

3.2 Certain services may not require CDD, however, in general, the Reporting Entity should take a cautious view when considering whether a particular matter falls within a transaction requiring CDD.

4 Different levels of CDD

4.1 The Regulation imposes various levels of due diligence obligations depending on the nature of the customer and the proposed professional relationship.

4.2 The Reporting Entity will assess whether the business relationship or occasional activity or transaction could involve money laundering or financing terrorism.

4.3 The Reporting Entity must assess the level of risk based on customer risk; country risk; service risk; and delivery risk in accordance with the Regulations. The First AML platform may be used to record this risk assessment.

5 Determining CDD requirements

5.1 The Reporting Entity will instruct First AML when it requires CDD to be conducted and must provide details of the person(s) requiring CDD for a customer.

5.2 First AML will determine the specific CDD requirements for the person(s) to whom CDD is required in respect of the customer, including the names of the beneficial owners.

5.3 The Reporting Entity will provide First AML with a customer contact so First AML can liaise directly with the customer if necessary to obtain the information required to determine the CDD requirements. First AML cannot, and shall not be obliged to, provide the Services if no customer contact satisfactory to the Service Provider is provided.

5.4 If agreed in writing First AML may collect evidence of source of wealth or funds if required by the reporting entity.

5.5 The Reporting Entity (and not First AML) is solely responsible and liable for determining if the evidence of source of wealth or funds is acceptable and in accordance with its Compliance Programme and the requirements of the AML/CFT Act.

6 Identity verification

6.1 First AML will carry out such necessary steps to conduct identity verification for all required individuals on behalf of the Reporting Entity.

6.2 First AML may use electronic identity verification or documentary identity verification to verify the identities of individuals in accordance with the AML/CFT Act.

6.2.1 When electronic identity verification is used, First AML confirms identities using electronic sources and includes additional measures for ensuring the identity document provided by the customer belongs to the customer and it has not been forged, altered or tampered with. Those additional measures include matching the individual to the identity they are claiming via a biometric comparison of a self-portrait photograph of the individual with the photograph on their identity document. The biometric comparison conducted by First AML involves analysis of the relative size, shape and position of the individual's eyes, nose, cheekbones, and jaw. First AML will record a pass/fail result after this analysis has been conducted. The assessment also involves analysis of the photograph of the identity document to look

for signs of forgery or alteration (e.g. discolouration, photograph layering, presence of watermarks and holographs etc.).

6.2.2 The electronic sources used are outlined in the 'Electronic Sources Schedule' in this document

6.2.3 When electronic verification is used First AML verifies an individual's name, date of birth and/or address. To achieve a pass, it checks name and date of birth and name and address. Under this approach the individual's name, date of birth and address at least once.

6.2.4 When documentary identity verification is used, First AML will request original copies of an individual's identity document (e.g. Passport) and proof of address (e.g. Utility Bill), please refer to First AML's Standard operating procedure for certification standards. If scanned copies of an individual's identity documents are sent instead of original copies, First AML may still verify the individual's identity.

6.3 First AML will liaise directly with the customer contact and/or customer individuals to obtain the necessary personal information to complete identity verification.

6.4 The Reporting Entity, (and not First AML), is responsible for making its assessment as to whether an individual or entity that it wished to enter into a business relationship with is of low, medium or high risk and will decide in its own right if more sophisticated measures should be applied to identify, or if a business relationship should be commenced with, such individuals or entities. First AML shall have no liability to the Reporting Entity with any such assessment made by the customer under clause 6.4.

6.5 First AML will also conduct PEP (Politically Exposed Person) checks on individuals in accordance with the Regulations.

6.6 When identity verification is complete First AML will inform the Reporting Entity via email so that it can, subject to compliance with its compliance programme and the Regulations, commence work for the customer.

7 Reporting

7.1 First AML will provide all information during and after customer due diligence and identity verification is conducted. This information is stored by First AML in the First AML Platform. The Reporting Entity will have access to this information.

7.2 The Reporting Entity is required to submit an annual report to the Regulators.

7.3 First AML can assist with the annual reporting process by providing information to the Reporting Entity on request.

8 On-going CDD and account monitoring

8.1 The Reporting Entity (and not First AML) shall be responsible and liable for monitoring its customer relationships on an ongoing basis, to:

8.1.1 Ensure that the transactions being conducted by a customer are consistent with the Reporting Entity's knowledge of the customer;

8.1.2 reassess risks; and

8.1.3 Update the Reporting Entity's CDD information and risk assessment where appropriate

8.2 The Reporting Entity will inform First AML if further CDD should be conducted (e.g. if there has been a change in the nature or purpose of the business relationship).

8.3 The Reporting Entity (and not First AML) is responsible for assessing its customer's transactions and activities and if necessary filing Threshold Transaction Reports and Suspicious Activity Reports.

Electronic Sources Schedule

First AML uses a 3rd party Electronic Verification provider Frankie Financial Pty Ltd ("FrankieOne") which has access to the electronic sources outlined in this schedule. These electronic sources are considered reliable and independent and will be used to verify the Name, Date of Birth and Address of verified individuals. Additional electronic sources may be added at any time. Onfido is used to perform biometric verification and document validity checks.

FrankieOne (Electronic Identity Verification Provider)

Accuracy	Real-time connection. Standard matching using exact Given Names, Surname, Date of Birth, residential address, ID number and expiry date (where applicable)
Security	All checks are done via a secure connection with the underlying database provider. FrankieOne is ISO/IEC 27001 compliant and is required to conform to ISO/IEC 27001 security protocols.
Privacy	As per FrankieOne's Privacy Policy, only a Pass/Fail response on each element is passed back to First AML. FrankieOne will not present First AML with additional information, such as the customer's correct Date of Birth but where possible will highlight which part of the check failed.
Method of information collection	Information is either entered by the relevant government body, updated by the relevant authorised bodies when information is changed or maintained by the credit bureau.
How the information is maintained	Maintained by each underlying data source provider individually or by the relevant credit bureau.
Whether the information has been additionally verified	Information may be held with the relevant government agencies, data consortiums and/or credit bureaus. Name, Date of Birth, address and ID number (where applicable) may be verified using additional databases.

Onfido (Biometric Verification and Anti-tampering Check Provider)

Accuracy	Real-time connection. Onfido uses different machine learning models and human-powered processes that are used to verify the identity or perform a check.
Security	Onfido is SOC 2 Type II compliant, and is certified by BSI to ISO 27001 under certificate number IS 660122. Onfido uses 256-bit SSL encryption 100% of the time on every device.
Privacy	As per Onfido's Privacy Policy, Onfido performs several electronic checks to determine whether the individual is a biometric match and if a document is genuine. Results are marked as either "approved" or "declined" or 'consider'.

Method of information collection	Onfido collects users' information from clients or directly from the users themselves. This information might include an image or images of an identity document (e.g. a passport or a driver's licence), photos (at times, taken in quick succession for anti-fraud purposes) or a video of the user, and the biometric facial identifiers extracted by Onfido from those images. Onfido also collects information about compromised identities that have been leaked or otherwise made available on the internet to further combat fraud. Lastly, Onfido will collect IP addresses to determine the city and country in which a user is located so that we may provide them with a localised service, where required to meet our legal obligations. They may also consider whether the IP address has been manipulated or shows unusual usage patterns.
Mechanism to link the person to the claimed identity	When conducting electronic identity verification, Onfido always incorporates its mechanism for linking the person to the claimed identity via a biometric facial recognition video that compares the photo or video provided by the applicant to the face on the document provided. Anti-tampering and fraudulent document checks are conducted in conjunction.
How the information is maintained	Maintained by Onfido
Whether the information has been additionally verified	Onfido is the only party that holds and maintains this information and therefore cannot be verified with an additional party.

ComplyAdvantage (PEPs, Sanctions, and Adverse Media)

Accuracy	Real-time connection. Matched against the full name (Including alias names) in both original and Latin script (where different), date of birth, citizenship/nationality, and address. All beneficial owners are screened against sanctions, PEPs (both foreign and domestic), warning if needed, fitness & probity databases and adverse media worldwide. Additionally, it screens all beneficiary details against sanctions, if needed also PEPs (both foreign and domestic), warning, fitness & probity databases and adverse media worldwide.
Security	All checks are done via a secure connection with the underlying database provider.

Privacy	Will record a Pass, Possible Match or Fail response. Further information will be provided if there is a Possible Match or Fail on the individual check.
Method of information collection	ComplyAdvantage aggregates hundreds of data sets. These data sets are updated daily. Sanctions sources are updated by ComplyAdvantage within 15 minutes of the sanctions lists being updated on the source.
How the information is maintained	Maintained by ComplyAdvantage. Please refer to this data overview for more information.

Full KYC/CDD Datasource List
FrankieOne and ComplyAdvantage's comprehensive data source list is linked here.

Please contact First AML If you require further information regarding these sources.