CUSTOMER DUE DILIGENCE OUTSOURCING TO FIRST AML

1 Introduction and Overview

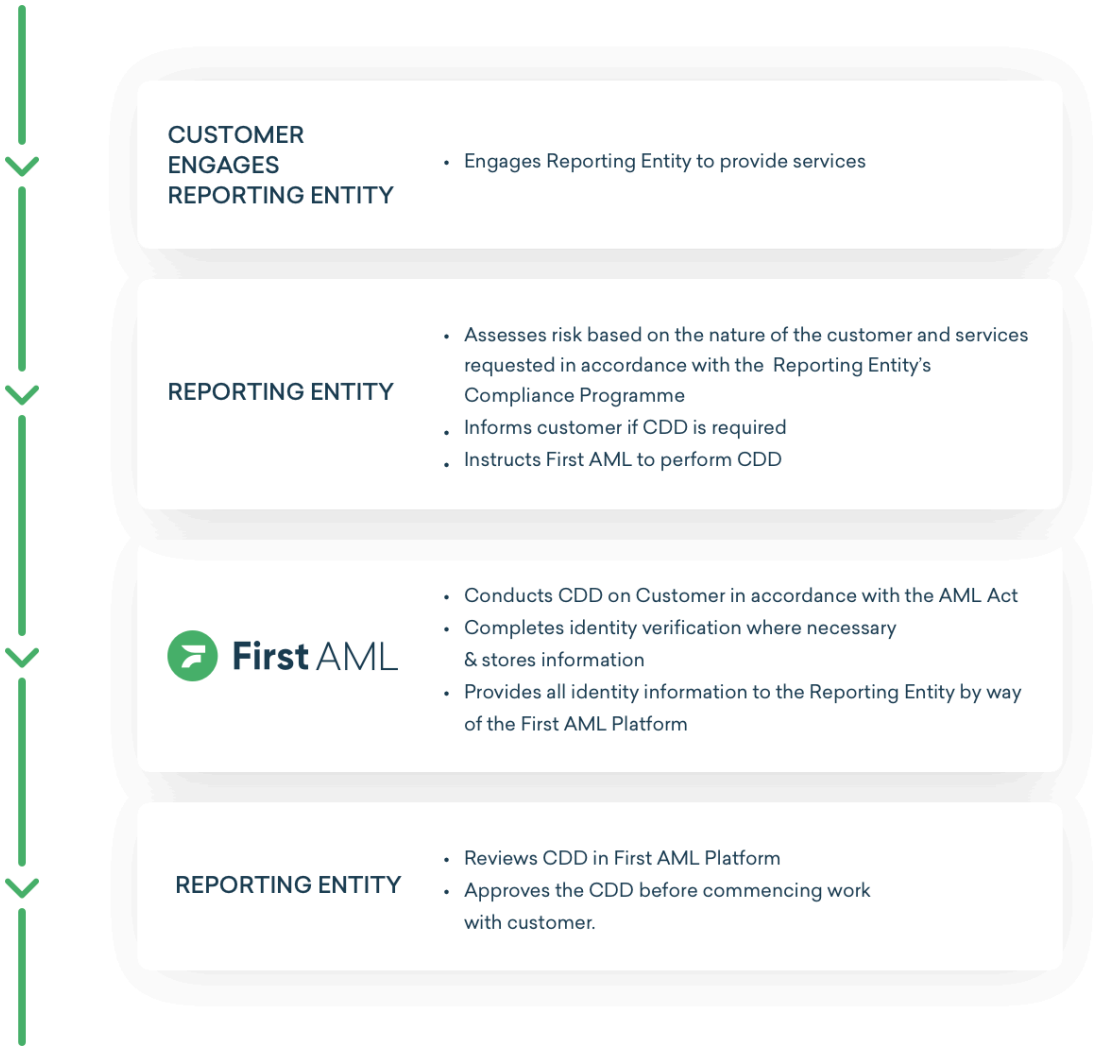
1.1 First AML provides an information and identity verification and workflow management Platform ("First AML Platform") to assist First AML customers ("Organisation") in verifying their clients ("Client") for their CDD (Customer Due Diligence) obligations in accordance with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 and its amendments ("AML Acts").. The First AML Platform is operated by the Organisation and First AML and the final decision to onboard a Client rests with the Organisation.

1.2 First AML may also act as a specialised CDD service provider operating as an agent of the Organisation in accordance with s34 of the AML Acts.

1.3 First AML conducts CDD on behalf of the Organisation, liaising directly with its Clients to perform the necessary verifications under the AML Acts (refer to Figure 1 for an overview). First AML will conduct CDD in line with First AML's Standard Operating Procedure unless agreed otherwise.

1.4 This document outlines how the platform operates, and how CDD is conducted when outsourcing to First AML and sets out the responsibilities of the Organisation and First AML. It does not provide all the necessary information required to be included in the Organisation's Compliance Programme or policies in respect of its compliance with the AML Acts.

Figure 1: Overview of the CDD Process



2 When CDD measures will be applied

2.1 As per s14, s18 and s22 the Organisation will apply CDD measures to a client whenever:

(a) it establishes a business relationship with the client:
(b) it carries out an occasional transaction for the client:
(c) it carries out an occasional activity for the client:
(d) there has otherwise been a material change in the nature and purpose of the business relationship:
(e) it considers that it has insufficient information about the client: or
(f) as soon as practicable after it becomes aware that an existing account is anonymous,

2.2 As per s17, s21 and s25 the Organisation 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 Organisation to be 'Captured Activities' (as defined in the AML/CFT Act).

2.4 This applies when an Organisation is required to take any measures under s14, s28 and s22 of the AML/CFT Act.

(a) Except as provided in subsection (b), an Organisation must carry out verification of identity before establishing a business relationship or conducting an occasional transaction or activity.
(b) Verification of identity may be completed after the business relationship has been established if:
    (i) it is essential not to interrupt normal business practices, and
    (ii) money laundering and financing of terrorism risks are effectively managed through procedures of transaction limitations and account monitoring or (if the Organisation is not a financial institution) through other appropriate risk management procedures, and
    (iii) verification of identity is completed as soon as is practicable once the business relationship has been established.

3 Capture

3.1 The Organisation is responsible and liable for determining if the services required by the client are transactions that require CDD.

3.2 Certain services may not require CDD, however, in general, the Organisation 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 AML Acts imposes various levels of due diligence obligations depending on the nature of the client and the proposed professional relationship.

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

4.3 The Organisation must assess the level of risk based on client risk; country risk; service risk; and delivery risk in accordance with the AML Acts.

5 Determining CDD requirements

5.1 The Organisation will create a case in the First AML Platform when it requires CDD to be conducted.

5.2 First AML is not responsible for determining the final risk or due diligence level of the Client.

5.3 First AML will determine the specific CDD requirements for the person(s) to whom CDD is required in respect of the client, including the names of the beneficial owners in line with the Standard Operating Procedure.

5.4 The Organisation will provide First AML with a client contact so First AML can liaise directly with the client 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 client contact satisfactory to the Service Provider is provided.

5.5 If agreed in writing First AML may collect evidence of the Client's source of wealth and/or funds if required by the Organisation.

5.6 The First AML Platform will facilitate the identification of the person(s) of whom CDD is required (using databases noted in Appendix 1). This may not determine all individuals needing verification in all instances. If, for example, they are outside of the reach of said databases for whatever reason (e.g. a Trust, any company data not made public to the KYB tool etc).

5.7 The Organisation will seek any additional information required based on their knowledge of their Client and ensure the more comprehensive risk profile is understood. The First AML Platform helps to form part of that picture.

5.8 It is the responsibility of the Organisation to determine if the source of wealth/funds evidence or other documentation provided by the client is acceptable.

6 Identity verification

Electronic sources are outlined in Appendix 1 of this document. The First AML Platform will conduct electronic identity verification on individuals in Australia, New Zealand and, to the extent the database list allows, further abroad. Please refer to the data sources list for a full list of data sources per country.

6.1 The First AML Platform will conduct identity verification for the relevant person(s) dictated by either itself or the client.

6.2 First AML will electronically verify identity information as per information input. If the identity verification fails electronically or if First AML does not have access to the government ID database to verify an individual's identity, supporting documents e.g. certified IDs may be requested through the Platform.

6.2.1 The First AML Platform verifies the identities of individuals using electronic sources as well as undertaking additional measures for ensuring the identity document provided by the client belongs to the client and has not been forged, altered or tampered with.

6.2.2 Additional measures include matching the client to the identity they are claiming via a live biometric image or video comparison which uses industry-leading algorithmic matching. The Organisation may opt to turn off the anti-tampering and biometric check at any time. The First AML Platform will record a pass/consider/suspected/rejected/fail result after conducting this analysis.

6.2.3 The Organisation may also use the 'met-in-person' function. If the Organisation meets the Client in person, they may opt to skip the biometric check in the form and collect the identity document electronically if desired. By using the met-in-person function, the Organisation (not The First AML Platform) confirms the identity document is of true likeness to the client and is an original document.

6.2.4 When electronic verification is utilised, the First AML platform collects and verifies an individual's legal name, date of birth and/or current residential address. This is designed in accordance with legislative requirements.

6.2.5 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 are verified against reliable and independent electronic sources.

6.2.6 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 client contact and/or client individuals to obtain the necessary personal information to complete identity verification.

6.4 The Organisation, is responsible for making its assessment as to whether an individual or entity that it wishes 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 Organisation with any such assessment made by the client under clause 6.4.

6.5 If configured, First AML will also conduct PEP (Politically Exposed Person) checks, sanctions checks and adverse media checks on individuals and entities in accordance with the AML Acts.

7 Reporting

7.1 The First AML Platform will provide a complete overview of all documents collected. These documents will be securely stored on the First AML Platform and will be accessible to the Organisation. This information can be used to assist with any auditing and reporting activities.

7.2 The First AML Platform reporting feature is available to support the Organisation with a range of reporting needs.

8 On-going CDD and account monitoring

8.1 The Organisation shall be responsible for monitoring its Client relationships on an ongoing basis, other than ongoing monitoring which will be undertaken daily (if configured accordingly).

8.2 The Organisation 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 Organisation is responsible for assessing its client's transactions and activities and if necessary filing Threshold Transaction Reports and Suspicious Activity Reports.

9 Employee vetting, training and quality control

9.1 Vetting Procedures for First AML Staff:

a) Extensive background checks, including criminal record checks and reference verifications, are conducted before onboarding any employee.
b) Verification of staff qualifications, experience and expertise in AML/CFT compliance through multiple short and long-answer written questions, in-person interviews, AML and compliance competency tests and checks to ensure that they can provide accurate and reliable CDD services e.g. CAMS, ICA, CISSP.

9.2 Training Initiatives for First AML Staff:

a) Comprehensive three-month onboarding training on AML/CFT regulations, policies and guidance relevant to each jurisdiction and industry.
b) Ongoing regular monthly training sessions to keep staff updated on any changes in regulations or best practices.
c) There are clear and standardised Standard Operating Procedures for all key aspects of our services and operations, including onboarding, customer success, delivery, and support.
d) All employees undergo rigorous training according to our Standard Operating Procedures and playbooks, ensuring consistency and adherence to best practices.
e) Dedicated continuous learning and professional development initiatives and funding for employees. This is coupled with personalised annual training plans.

9.3 Quality control of CDD work:

a) Robust quality assurance measures are implemented to review and assess the accuracy of CDD reports generated by First AML.
b) Regular monthly audits and randomised spot checks are carried out to evaluate the performance of First AML staff and identify any areas of improvement. Any findings are required to be remediated within the week.
c) All cases are peer-reviewed by other First AML staff before sending to the Organisation for review to ensure each case adheres to the Standard Operating Procedure requirements.
    i) For any complex or high-risk cases identified, there are clear escalation procedures for additional review with a senior staff member.
d) Feedback and coaching are provided to all First AML staff on a weekly or fortnightly basis to address learnings and areas of improvement identified
e) All activities within the First AML platform are documented within the platform and stored securely

Appendix 1

Electronic Sources Schedule

First AML uses third-party Electronic Verification providers which have 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, to conduct anti-tampering and biometric checks on individuals, or to collect KYB information for entities. Additional electronic sources and subsets of existing data source providers may be added at any time.

For a complete list of our subprocessors please refer to our website page.

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 client'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 or 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), warnings if needed, fitness & probity databases and adverse media worldwide. Additionally, it screens all beneficiary details against sanctions, if needed as well as PEPs (both foreign and domestic), warning, fitness & probity databases and adverse media worldwide.
Security	All checks are done via a secure connection with the database provider.
Privacy	Will record a positive match or no match response. Further information will be provided if there is a positive match to determine whether it is a True or False Positive match.
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.
Whether the information has been additionally verified	The respective PEP, sanctions and adverse media lists are held and maintained by ComplyAdvantage. Certain sanction lists are pulled from publicly available sources e.g. OFAC, HM Treasury, DFAT, etc.

Kyckr (KYB Information Provider)

Accuracy	Real-time connection at the point of request. Kyckr searches publicly available corporate registries for matching records to the supplied company name and registration number. Company information is time and date-stamped at the time of retrieval with the name and logo of the relevant corporate registry.
Security	All checks are done via a secure connection with the database provider.
Privacy	Kyckr's software can transfer data including personal data, namely the details of directors and shareholders from the public domain to First AML via API.

	All data is transmitted from public registries which are official repositories of businesses that have been incorporated within a country and are accessible to anyone. No personal data is stored within Kyckr.
Method of information collection	Kyckr searches both individual corporate registries (in real-time) along with a cache of global registry data.
How the information is maintained	Maintained by the respective corporate registries.
Whether the information has been additionally verified	The respective corporate registries are the only party that holds and maintains this information and therefore cannot be verified with an additional party before being made available by the registry to third-party providers.

Centrix (Electronic Identity Verification Provider)

Please note this provider is only relevant to Organisations verifying individual clients based in New Zealand.

Accuracy	Real-time connection. First AML sends the Name, Date of Birth and Address to Centrix and returns a positive match if all details match using Centrix's matching algorithms. Middle Name is sent if provided. Address matching is performed by Centrix (no normalisation is performed byCentrix)
Security	All checks are done via a secure connection with the database provider.
Privacy	As per Centrix's Privacy Policy, only a Pass/Fail response on each element is passed back to First AML. Centrix will not present First AML with additional information, such as the client's correct Address
Method of information collection	Entered by the companies that supply data to Centrix, for example, a company that supplies monthly credit account (CCR) data or needs to run a credit check on their client.
How the information is maintained	Maintained by Centrix Group
Whether the information has been additionally verified	Centrix are the only party that holds this set of information and therefore cannot be verified with an additional party. However, name and address information can be additionally verified using other databases available within Centrix.

Equifax (Electronic Identity Verification Provider)

Please note this provider is only relevant to Organisations verifying individual clients based in the United Kingdom.

Accuracy	Real-time connection. First AML sends the Name, Date of Birth and Address to Equifax and returns a positive match if all details match using Equifax's matching algorithms. Middle Name is sent if provided. Address matching is performed by Equifax. The Equifax bureau data also undergoes ongoing data enrichment to support data accuracy. This enrichment occurs following the results of internal monitoring, as well as client and consumer feedback.
Security	All checks are done via a secure connection with the database provider.
Privacy	As per Centrix's Privacy Policy, only a Pass/Fail response on each element is passed back to First AML. Equifax will not present First AML with additional information, such as the client's correct Address
Method of information collection	Data is received from consumer credit providers, commercial credit providers, and public records. Data is refreshed daily in Equifax's real-time environments
How the information is maintained	Maintained by Equifax.
Whether the information has been additionally verified	Individual data is held by Equifax and can be validated against other credit bureaus. Various elements of the commercial bureau can be validated against public corporate registries.

Datasource List

First AML uses reliable and independent electronic data sources to verify KYC (Know-Your-Customer) and KYB (Know-Your-Business) information. Additional electronic sources may be added at any time.

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