

## Outsourcing your CDD requirements

An increasing number of DIA and FMA supervised reporting entities are outsourcing their customer due diligence (CDD) obligations to specialist AML third-party providers.

Typically, the outsourcing of CDD to the third-party provider occurs as part of a reporting entity's on-boarding procedures for its new customers. The third-party provider is not itself a reporting entity and is acting as the reporting entity's agent under section 34 of the AML/CFT Act.

Services provided by third-party providers may include looking through ownership structures of legal persons and legal arrangements to identify beneficial owners and persons acting on behalf of the customer. The provider then engages with these persons to verify their name, date of birth and address using electronic sources. Other services include obtaining information and undertaking verification of the source of funds or wealth of a customer. At completion, the third-party provider presents the reporting entity with a report detailing its findings.

While third-party providers can provide a useful service, both the DIA and FMA are aware of an increasing number of reporting entities taking a view that the third-party provider "just takes care of it all" and that all CDD requirements are then met. This is not the case.

### Relying on a third-party provider

Section 34 of the AML/CFT Act allows a reporting entity to authorise and rely on an agent to conduct CDD procedures on its behalf. An agent is a person that has legal authority to represent another party.

If you outsource the above CDD procedures under section 34 to a third-party provider, the provider must be acting as your agent. In these circumstances, you **remain responsible** for ensuring that the CDD conducted by the third-party provider is undertaken to the level required by the AML/CFT Act. It is also important to remember the following:

### Customer Due Diligence

- The parts of your CDD procedures that you outsource do not exist in isolation from your wider CDD and other obligations under the AML/CFT Act.
- These wider CDD obligations include a requirement that you obtain information on the nature and purpose of a proposed business relationship. This information needs to be considered alongside the type of service, activity or transaction to be provided to the customer, as well as the CDD undertaken by the third-party provider, to determine the level of risk and whether enhanced CDD is required. You may need to obtain further information from the customer so that this can be determined.
- As part of your ongoing CDD and account monitoring obligations, you must regularly review the CDD information you hold for a customer (including that undertaken by the third-party provider).

### **Record keeping**

- Your record keeping obligations require you to retain records of the data, documents or information from a reliable and independent source that was used for the purpose of identity verification. These records must be in a form that is readily accessible.
- If you are outsourcing CDD to a third-party provider that uses electronic identity verification, it is the underlying database used (and not the third-party provider) that is the electronic source.
- Your record keeping obligations continue even if you cease an outsourcing relationship with a particular third-party provider.

### **AML/CFT programme**

- All CDD policies, procedures and controls should be documented in your AML/CFT programme. This should include detailing the reliable and independent electronic sources used by your third-party provider.
- There should be controls and escalation procedures in place if verification to the level required by the Act cannot be met through the third-party provider.