**ACCA Client Due Diligence Member Factsheet**

Client due diligence (CDD) is an important measure available to accountants to prevent money laundering and avoid their practices being used by criminals to launder the proceeds of crime.

It is important to note that this factsheet should be read in conjunction with the client risk assessment factsheet.

The Criminal Justice Acts 2010 to 2021 outline the requirements that accountants must apply in respect of CDD. Accountants must be vigilant and practice good CDD.

Conducting CDD requires practitioners to collect and document information about their client’s personal background and business, this is often referred to as know your client information or more commonly ’KYC information’. Understanding the nature of a client’s business enables accountants to identify behaviours that appear to be unusual and may amount to suspicious activity when considered in context with what’s known about the client’s background. In order to understand the nature of a client’s business, practitioners must establish the following;

* the legal structure (sole trader, limited company etc.) of the business. A certificate of incorporation, breakdown of share ownership or a partnership agreement are examples of documents that can be reasonably relied upon to verify this.
* date of incorporation/date trading commenced.
* the identities of the ultimate beneficial owner(s), directors and other persons of significant control. This must be verified by taking a valid form of photo ID for each individual (i.e. passport or driving licence) and a valid proof of address. Documents typically accepted as a valid proof of address are a recent (i.e. issued within the last three months); utility bill linked to a fixed address, council tax statement, tenancy agreement, mortgage agreement/statement or a bank statement, there may be exceptional occasions where other documents not listed above may be acceptable as a valid proof of address and the details and rationale for accepting these should be fully documented.

Additional information will also be required when on-boarding all new clients in order to have a sound understanding of a client’s business i.e.;

* their source of income
* sector the client operates in
* previous years’ turnover and future revenue projections
* operational structure (i.e. the number of employees, geographical connections such as the location of any branches and offices etc.)
* if there is any adverse media associated with the client, best practice is to search the client’s registered name, trading name (if different) and the names of the client’s ultimate beneficial owners/directors in an internet search engine to check whether any relevant results are returned, following this it is advised that these names are searched in combination with key words such as; money launder, arrest, custody, jail, prison, fraud, trial, tribunal, hearing and any other words that may be relevant to performing a targeted adverse media search on the client
* an understanding of key business partners and suppliers where applicable.

This information must be recorded concisely in a document for quick and easy reference, such as a KYC form, please refer to the KYC form and client risk assessment tool document

You should also consider documenting what evidence of KYC you would not accept. For example, a driving licence shouldn’t be used as both a form of photo ID and a proof of address. Provisional driving licence, mobile phone bills or credit card statements are not typically considered to be acceptable either. Photos of identification sent into the firm by the client that is not independently verified would not typically be considered an acceptable form of identification.

In cases where it is not possible to meet a client face-to-face, it will be necessary to strengthen the on-boarding process with additional EDD measures to ensure the risk is managed. For example, a video call session to verify photo ID or an additional form of ID. These measures are particularly relevant to managing remote client engagements effectively.

Reliance on third party software

In some cases, practitioners may choose to rely on third party software to assist them when conducting CDD. It is important to point out that the use of third-party software cannot be relied upon as a substitute for gathering CDD information and obtaining copies of ID, proof of address and other supporting documents first-hand from clients. It may however be best to enhance the CDD process for high risk clients, to verify information about their identity against information kept on public records such as; sanctions list, PEP status and adverse media. Practitioners must have a sound understanding of what the software’s features are and what jurations it is applicable for, to ensure it is suitable for their purposes before they commence using it. For example, if the software validates a passport number – does it just check the passport number is following the right format or that that specific passport number belongs to the correct person? Does the software pick up Irish PEPs or does it only identify UK PEPs. The software should be secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.

Pre client onboarding

Prior to entering into a business relationship with a new client, a practice must do a search of RBO (Register of Beneficial Owners) and confirm that the beneficial ownership details are consistent with their understanding. Short videos on how to search the RBO details for a new client are at this [link.](https://www.rbo.gov.ie/how-to.html)

If the new client is not on the register, then the practice should report them using a [non-compliance notification](https://rbo.gov.ie/images/NCN_Form.pdf)  form. If the beneficial ownership details are wrong, then a discrepancy notice is filed. A DN2 form is filed for a discrepancy and this form is available to the practices RBO Liaison Officer (who will probably also be the practices anti-money laundering reporting officer) by contacting discrepancies@rbo.gov.ie The full filing procedure for a discrepancy form is at this [link](https://www.rbo.gov.ie/faqs/reasons-for-rbo-beneficial-owners-submission-rejection.html).

The rules were brough in for corporate clients by [European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019](http://www.irishstatutebook.ie/eli/2019/si/110/made/en/pdf) and trust clients by [European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) Regulations 2021](http://www.irishstatutebook.ie/eli/2021/si/194/made/en/pdf)  Trusts have 6 months from 24 April 2021 to upload their details for the first time to the RBO. Corporate entities had until 22 November 2019 to upload their details.

Enhanced Due Diligence

In scenarios involving high risk clients, it will be necessary to conduct additional due diligence to mitigate the higher level of risk associated with the client, this is something referred to as enhanced due diligence (EDD). In addition to the information collected above, EDD measures often include, but are not limited to the following measures;

* obtaining an additional method of photo ID
* obtaining proof of funds/wealth
* visit client onsite at their business premises to verify it is consistent the information provided
* verifying client information with a reliable third-party, i.e. Companies Registration Office or other reputable third-party information providers
* taking steps to understand the business activities of beneficial owners that are commercial entities

On-going monitoring

Practitioners must ensure the KYC information they hold in relation to their clients is up to date and relevant, to do so firms will have to conduct on-going monitoring on their clients. This process involves refreshing KYC information periodically. Using a risk-based approach, practitioners must ensure that the KYC information of their high-risk clients is reviewed and updated if necessary more frequently - e.g. at least every 12 months. In addition to this, there may be times where CDD records must be updated prior to the periodic review date due to a significant change in circumstances such as a change in ownership or adverse is commonly referred to as an ‘Event Driven Review’. For accountants to maintain a good understanding of their client, they will need to confirm the following information as part of their on-going monitoring;

* has there been any change in ownership? This can be best achieved by consulting Companies Registration Office and/or the Register of Beneficial Ownership.
* are all photo IDs up to date?
* has there been any change in the nature of the client’s business (e.g. diversification into a new sector or market)?
* is there a change to the intended purpose of the engagement?
* are there any new links to international jurisdictions?

has there been any significant changes in the level of client’s turnover?

* Have there been any large transactions made recently?
* Are future business plans inconsistent with the client’s background, or do they make little commercial sense?

If the answer is yes to any of the above considerations, then this should be understood and documented on the client CDD file the explanation makes little commercial sense or appears suspicious then it may be necessary to file a SAR or reclassify the client as a risk.

On-going monitoring carried out by a firm must be documented and recorded, in a similar fashion to the KYC information that is captured at the point of initiating the business engagement. An example KYC form can be found in the ‘Client Risk Assessment Tool and KYC form. You should document even if there have been no changes, to evidence that on-going monitoring is taking place. Please note that the lists in this article are not exhaustive and different variations of these questions, as well as other additional questions may be necessary for specific types of clients. You should keep up to date with new legislation requirements. You should also be aware of emerging risks and trends in relation to financial crime.