Technical factsheet

Customer due diligence

Customer 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 ACCA's client risk assessment factsheet.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 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 (ie passport or driving licence) and a valid proof of address. Documents typically accepted as a valid proof of address are a recent (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; the details and rationale for accepting these should be fully documented.

Additional information will also be required when onboarding all new clients in order to have a sound understanding of a client's business, ie:

- their source of income
- sector the client operates in and trading activities
- previous years' turnover and future revenue projections

- operational structure (ie 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
- check for any discrepancies between the information provided to you by your clients concerning their beneficial ownership and the person of significant control register recorded with Companies House. Any discrepancies identified must be reported to Companies House.

This information must be recorded with sufficient detail, so it is clear to those within the practice and also a third party (such as your AML supervisor or law enforcement) what was done and when. It should be recorded in a document for quick and easy reference, such as a KYC form. Please refer to ACCA's client risk-assessment tool and know-your-customer form for an example.

You should also consider documenting what evidence of KYC you would not accept. For example, a driving licence should not 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 onboarding process with additional enhanced due diligence (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, politically exposed person (PEP) status and adverse media.

Practitioners must fully understand the software's features to ensure it is suitable for their purposes before they commence using it. Practitioners should be able to explain how the software meets the requirements set out in the firm's AML policy and procedures, and how it addresses and helps manage the firm's specific AML risks identified in their firm-wide risk assessment. For example, if the software validates a passport number, does it just check the passport number is following the right format or does it confirm that specific passport number belongs to the correct person? Does the software retain copies of ID documents that are

scanned into the system and can the practitioner retrieve these, or is the software reliant on the practitioner manually entering the relevant ID number?

Practitioners should always be able to provide evidence of what ID has been input into the third-party system. They should not rely on a printout to say a search was done on a particular date without being able to supply evidence of the underlying documentation used to conduct that search.

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.

Enhanced due diligence (EDD)

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 referred to as EDD. It is particularly important to conduct EDD in situations involving transactions that are complex, unusually large or there are unusual patterns of transactions, as well as transactions that have no apparent commercial or economic purpose. Firms must also ensure that they conduct EDD on all clients based in, trading with or transacting to a high-risk third country as defined by the Financial Action Task Force (FATF). 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
- obtaining invoices, sales records and receipts to ensure that revenue figures and business expenses are credible, and that sales and purchases are made from legitimate sources
- visit client onsite at their business premises to verify that it is consistent with the information provided
- verifying client information with a reliable third party, ie Companies House or other reputable third-party information providers
- taking steps to understand the business activities of beneficial owners that are commercial entities.

Ongoing monitoring

Practitioners must ensure that the KYC information they hold in relation to their clients is up to date and relevant. To do so, firms will have to conduct ongoing monitoring. 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 – eg 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 media; this 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 ongoing monitoring:

- Has there been any change in ownership? This can be best achieved by consulting Companies House. It is important to note on this point that an aspect of the newly transposed Fifth Money Laundering Directive obliges accountants to inform Companies House if there is a discrepancy between the information that they hold about a beneficial owner of a company, limited liability partnership or Scottish limited or qualifying partnership and the information that is on the person with significant control (PSC) register.
- Are all photo IDs up to date?
- Has there been any change in the nature of the client's business (eg 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?
- Have there been any significant changes in the level of client's turnover?
- Have any large transactions been 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. If the explanation for changes makes little commercial sense and appears suspicious, then it may be necessary to file a SAR or reclassify the client as a higher risk.

Ongoing 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 ACCA's client risk-assessment tool and know-your-customer form. You should document even if there have been no changes, to evidence that ongoing 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.

October 2022