Think Ahead ACCA

Technical factsheet

ACCA client due diligence

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

It is important to note that this factsheet should be read in conjunction with ACCA's *Technical factsheet: identifying client risk*.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) outline the requirements that accountants must apply in respect of CDD. Accountants must be vigilant and practise 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 (KYC) information. Understanding the nature of a client's business enables accountants to accurately risk assess their clients and identify behaviours that appear to be unusual, which may amount to suspicious activity when considered in context with what's known about a 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 on to verify this.
- Date of incorporation/date trading commenced.
- The identities of the ultimate beneficial owner(s), directors and other persons of significant control or influence. These will vary depending on the type of entity the client is. For example, for a limited company a beneficial owner will be any individual who has a shareholding of 25% or greater; for a partnership, a person named as a partner within a partnership agreement will generally meet the definition of a beneficial owner. For a trust, a person of significant influence could be a trustee, settlor or beneficiary, depending on who actually exercises significant influence or control over the activities of that trust.
- Verifying the identifies of ultimate beneficial owner(s), directors and persons of significant control or influence must be undertaken by taking a valid form of photo ID for each individual (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 past 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. Please refer to the UK government's proof of identity checklist for further information.

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

- overview of the client's trading background and history, including how the business was established
- detailed description of the client's trading activities, including core products, goods and/or services, and how they are produced, delivered or traded
- an understanding of key business partners, stakeholders and suppliers where applicable
- previous years' turnover and future revenue projections
- the source of any startup capital and investment funds used to set up the business
- operational structure (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 ultimate beneficial owners/directors in an internet search engine. 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
- where applicable, any relevant international or crossborder links the client may have, particularly with respect to high-risk third countries
- check for any discrepancies between the information provided by your clients concerning their beneficial ownership and the person of significant control register recorded within Companies House. Any material 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 CDD has been completed on clients and when. All CDD checks and KYC information gathered should be documented for quick and easy reference.

CDD files will often comprise onboarding checklists, client risk assessments, KYC forms, ID verification forms, ongoing monitoring reviews and supplementary data. Please refer to ACCA's KYC form and client risk-assessement tool document for an example of what an initial onboarding form is generally expected to consist of.

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. Photos of identification sent into the firm by the client that are not independently verified would not typically be considered acceptable.

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. These measures will need to be included within your firm's AML policy and procedures to ensure that they are correctly and consistently applied by all members of staff.

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 that does not include biometric checks, and only requires practitioners to input their client's name, date of birth, address and other personal data, cannot be relied on as a substitute for gathering CDD information and obtaining copies of ID, proof of address and other supporting documents first-hand from clients.

CCAB guidance states that *'before using any electronic service, firms should ensure they understand the basis of the systems they use and question whether the information is reliable, comprehensive and accurate. The process 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, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing.'*

It is therefore ACCA's position, in line with this guidance, that firms must obtain and review photographic identification to achieve this level of assurance concerning authenticity. As noted by CCAB, sole reliance on electronic verification software is insufficient, as this typically only confirms that an individual with a given name and date of birth exists, rather than verifying that the individual presenting themselves is that person.

However, the use of reliable third-party software to perform an additional verification check is an effective way to enhance the standard CDD process if concerns exist concerning a client's identity, sanction or politically exposed person (PEP) status. Please note that this does **not** apply to third-party verification platforms that require biometric checks to be completed whereby clients provide a live photograph or video of themselves alongside photographic identification in order to confirm likeness and authenticity, as these systems provide a higher level of identity assurance.

If third-party software is used, practitioners must fully understand the software's features to ensure that 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 its firm-wide risk assessment. For example, if the software validates a passport number, does it just check that the number is following the right format or does it confirm that that specific 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 inputted into the third-party system. They should not rely on a printout to say that a search was done on a particular date without being able to supply evidence of the underlying documentation used to conduct that search.

The bottom line is, 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 clients that have been risk assessed as high risk, 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 the following situations:

- clients that make or are involved in 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
- a business relationship with a client established in, or with links to, a high-risk third country as defined by the Financial Action Task Force and named in HM Treasury's Money Laundering Advisory Notice: High Risk Third Countries
- if a business has determined that a client or potential client is a foreign PEP, or a family member or known close associate of a foreign PEP
- in any other case which, by its nature, can present a higher risk of money laundering and terrorist financing.

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
- visiting the client at their business premises to verify that it is consistent with your knowledge of, and the information gathered and provided by, the client
- 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, within the range of every three years for normal-risk clients and every five years for low-risk clients at a minimum. 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 for all types of clients must be updated prior to the periodic review date due to a significant change in circumstances; this is commonly referred to as an 'event-driven review'. This may typically involve, although not be limited to, the following:

- a change in beneficial ownership or directorship
- unexpected or inconsistent transactions, such as significant surges in activity, large transfers or behaviour deviating from the established profile of the client

- a significant change in the type of business activity that the client normally undertakes – for example, operating within a new sector that it has no prior experience in, or commencing trade with international jurisdictions it previously had no connection with
- discovery of new or previously undiscovered adverse media reports
- a change of PEP status
- a change in the client's underlying risk assessment categorisation.

For accountants to maintain a good understanding of their client, they will need to confirm the following information as part of their ongoing monitoring that is reflective of the above outlined trigger events:

- Has there been any change in ownership? This can be best achieved by consulting Companies House. It is important to note 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?
- Has there been any significant changes in the level of the 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 it must also be documented on the client CDD file for audit trail purposes. If the explanation for changes makes little commercial sense and appears suspicious, then it may be necessary to file a suspicious activity report or reclassify the client as 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. ACCA has produced a KYC template to assist with this requirement. You should document when a review of a client's CDD file has taken place, even if there have been no changes, to evidence that ongoing monitoring is taking place on a periodic basis as required by MLR 2017.

Please note that the lists in this factsheet 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.

Expired identification documents

It is the responsibility of the money laundering reporting officer (MLRO) to implement an appropriate and consistent risk-based approach to ensure documentation, data and

information obtained for CDD purposes is kept up to date; the easiest and simplest approach is to update expired documents when identified during an ongoing monitoring review. If an MLRO adopts this approach, then this should be completed. If, however, you take an approach where, on a risk-based approach, you have identified that a document has expired but you do not deem there to be any risk so an updated document is not obtained, this should be fully documented, and this process should be included within your AML policy and procedures document.

Updated May 2026