Record Keeping

The EU Money Laundering Directive and the money laundering regulations require accountants in practice to retain records of specific information for a period of 5 years from the end of a business relationship or the completion of an occasional transaction. Such records include client due diligence information, information on suspicious activity reports made to the authorities, or suspicious activity which was reported internally by staff and subsequently not required to be reported to the authorities, having been analysed by the money laundering reporting officer (MLRO). Training records for all relevant staff must also be retained. A failure to keep records is an offence under the regulations.

Client due diligence (CDD) records

The EU money laundering directive and the national money laundering regulations obliges accountants to retain client due diligence records for a period of 5 years from the end of the relationship or the completion of an occasional transaction. Bear in mind that good record-keeping, could in the future, help to defend against a money laundering or a terrorist financing offence. Client due diligence records should include:

- client identification information
- copies of original documentation used for verification of identity
- information on the ownership and control structure of the client business;
- identification and verification information on any beneficial owners if applicable;
- information and records on the purpose and nature of the relationship;
- records of having conducted ongoing monitoring of the relationship and client activity.

Information on the nature of the business relationship such as Terms of Engagement, client statements/submissions/requests, records of accounts/transactions and size, volume or frequency of services done should be retained and readily recovered if needed. This could also include records of any email or written correspondence (i.e. non-engagement documentation).

If the client is or has been assessed as a higher risk, evidence of enhanced due diligence procedures including evidence of additional controls and evidence must also be recorded. This would include, for example, records of additional identification evidence, additional documentation on the source of wealth/ income, certified copies of identification documents or additional information to verify the ownership and controls structure of the client and so forth.

If you intend to rely upon the client due diligence checks of another AML regulated person/body, it is your responsibility to ensure that you have a record of that third party’s consent allowing you to rely upon their CDD checks. Ultimate responsibility for meeting CDD requirements shall remain with the party who is relying on the third party.

Records of suspicious activity reports (SAR)

It is important that your practice has a formal written policy in respect to the recording of information surrounding internal reports of suspicious activity made by staff to the MLRO, and subsequently by the MLRO to the authorities. At a minimum, this policy should include a format for describing the suspicion/knowledge and who is involved, name of who is to receive the report within the practice (eg.
MLRO), any timelines for actions to be taken and responsibility of the MLRO to acknowledge receipt of the report and to warn the reporter about the ‘tipping-off’ offence.

The MLRO must detail and record the actions/decisions taken arising from the analysis of a report which he or she has received from a staff member. The MLRO must record all decisions and reasons for how the report was responded to, or how the decision to report or not to report externally to the authorities was reached. Such information regarding the internal and external reports and the outcome, if any, must be recorded on file for 5 years. The record of the suspicious activity report or investigation should be kept separately from the main client file. This is a safeguard against an unwarranted or accidental disclosure which could result in prejudicing an investigation or committing the ‘tipping-off’ offence.

Training records
The training of staff is a significant factor for defeating money laundering or terrorist financing and you should be able to prove that all staff are aware of the law and their personal obligations. A failure to provide training to all relevant staff is an offence.

Records of training provided/received should include the recording of attendance lists at training sessions, staff declaration of awareness of the law/regulations, filing of training manuals, records of training for new staff to show they are aware of the practice’s internal policy and the ML laws or regulations. It is common for professionals to give training on AML/CTF to staff without any formal record being taken (eg. ‘On-the-job training’). If training is given on the job then the trainer should make a note of what was covered in the session and sign and date that record. If you cannot produce records of employee training, for example there may be no defence against a prosecution for failing to report a suspicion of ML/TF.

General records of internal AML controls
More generally, it is important that you record the reasons and basis for any actions or decisions taken surrounding your practice’s overall risk-based approach to AML/CTF compliance. Record-keeping duties should extend to your general AML/CTF internal policies and procedures adapted by your practice and these could for example be in the form of an internal AML/CTF policy document. In preparing a practice risk assessment, you are determining the risk profile of your practice and you must be able to explain the reasoning behind how you decided your practice’s risk profile and to explain how you responded to these risks.

Good records of client activity and client due diligence, will allow you to assist law enforcement or the authorities in any investigation which may arise. Good records are also important to enable you to demonstrate compliance with your regulatory and legal obligations should CIMA conduct an on-site AML supervision visit.

Format of record-keeping
- Original documents
- Photocopies or scans of original documents
- Computerised or electronic form records
- Electronic files or hard copies of the results of electronic/subscription services checks carried out

Disclaimer: Whilst every effort has been made to ensure the accuracy of the information in this document, it does not constitute legal advice and cannot be relied upon as such. CIMA does not accept any responsibility for liabilities arising as a result of reliance upon the information provided in this document.