Covid-19 and preventing Money Laundering/Terrorist Financing in Legal Practices

15 April 2020

The Legal Services Affinity Group, of which the SRA is a member and includes regulators across the UK, has drawn up more detailed guidance below on dealing with anti-money laundering compliance during the coronavirus pandemic.

Legal Sector Affinity Group (LSAG) – Advisory Note

Legal practices and practitioners should be aware that criminals will continue to operate throughout, and look to take advantage of, the Covid-19 outbreak. This includes laundering the proceeds of crime and terrorist financing, so it is important that everyone is aware of the changing risks.

Legal Sector Anti- Money Laundering (AML)/ Counter-Terrorist Financing (CTF) supervisors understand the particular challenges currently facing legal practices and practitioners. This includes the difficulties associated with undertaking customer due diligence (CDD), including appropriate levels of identification and verification (ID&V) – particularly where clients cannot be met face-to-face.

Please note legal practices and practitioners in scope of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (the MLRs) must still comply with their statutory requirements at all times.

However, in line with a risk-based approach, the MLRs provide flexibility in the application of their requirements. There exist options for practices seeking to comply while also observing requirements such as social distancing.

Risks that may arise due to Covid-19

As well as changes to how we live our lives, Covid-19 is also changing the economy. An economic downturn may make legal practices more susceptible to financial difficulties or other pressures, which creates risk and potential weaknesses for criminals to exploit. As the UK economy enters a period of uncertainty, practitioners and practices should be particularly alert to the following risks in new or prospective customers:

- Being asked to work with unusual types of client or on unusual types of matter
- Resistance from a client regarding compliance with due diligence checks, for example being pressured to forego necessary due diligence checks or to "speed up" the process.
- Becoming involved in work that is outside of the practice's or practitioner's normal area of experience/expertise – without full understanding of the money laundering and counter terrorism risks associated with the new area of work
- Any attempt to gain access to your client account where not accompanied by the provision of legal services
- Transactions where the business rationale for the transaction is not clear.

Always ensure that you are comfortable as to your understanding of the matter, including its

purpose and why it is happening in the particular way it is happening.

Identification and Verification

ID&V, is often undertaken in person, on the premises of the legal practice using suitable identification documents. This can provide a strong level of assurance, but this may no longer be possible in the current circumstances and you should consider what risks this may create.

An inability to conduct in person ID&V does not mean you cannot complete CDD, but you may need to consider using other methods that give you the necessary assurance that the person is who they say they are.

Practices and practitioners are reminded to adopt a risk-based approach, taking into account the contents of their practice-wide risk assessment, policies and procedures (and where necessary updating them) and the circumstances of individual clients/matters. As an alternative to face-to-face documentary verification, legal practices and practitioners may adopt or further utilise electronic means of ID&V where appropriate to the risks present in the client/transaction.

Such methods may include (but are not limited to) using independently or in combination:

1. Digital ID&V services that meet the requirements of the MLRs (R28(19) - "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.")
2. Gathering and analysing additional data to triangulate the evidence provided by the client, such as geolocation, IP addresses, verifiable phone numbers etc.;
3. Verifying phone numbers, e-mails and/or physical addresses by sending codes to the client's address to validate access to accounts
4. Using live and/or recorded digital video (many reliable and free options exist for this) of the customer showing their face and original photo identification documents so that you can compare them to a scanned copy of the same document (e.g. passport or driving license).

No matter what ID&V service or procedure is used, the responsibility to make sure the ID&V is undertaken correctly, is with the relevant practitioner and practice. If you are placing reliance on others to conduct CDD under Regulation 39, e.g. an instructing solicitor or accountant, you should ensure that you understand how they have adapted their CDD procedures to the different circumstances.

Make sure that you keep a record and evidence of the processes you follow; for example, of any video calls you make.

These methods alone may not be appropriate or sufficient where the money laundering and terrorist financing risks inherent in the particular client or matter are greater. In higher risk situations, further verification (including verification of source of funds/wealth) will likely be required.

Where you need to update ID&V records for existing clients, you should not rely on old ID just because you cannot currently meet them face-to-face.

Further, information and advice may be available on your Supervisors website. You are also referred to the HM Treasury approved LSAG Anti-Money Laundering Guidance for the Legal Sector (March 2018) and LSAG Key Changes Document issued January 2020.

Digital Identification and Verification Services

If you are considering whether to use a digital ID&V service, you must carefully consider whether it provides the assurance needed. In order to make this judgement, you may have regard to the Financial Action Task Force (FATF) guidance on Digital Identity (PDF 107 pages, 4.1MB) [https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf] , particularly recommendations 22-27 in the Executive Summary (PDF 8 pages, 347KB) [https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf] as summarised below.

1. Understand what the service actually does i.e. what checks is it doing and what databases is it checking, if any.
2. Take a risk-based approach to relying on the service including understanding the assurance level provided and that it is appropriate to the risk.
3. Understand whether the service provides levels of assurance and how these may be appropriately used in different circumstances.
4. Consider whether using the service, negates the idea that all non- face to face transactions are high risk.
5. Use anti-fraud and other cyber security processes to support the service.
6. Engage with the service provider to ensure the practice has access to the information it may need to prove its compliance to its supervisor or to law enforcement.

Another important consideration is whether the service has attained any accreditation or certification from any of the bodies listed in Appendix D of the FATF guidance (PDF 3 pages, 235KB) [https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Appendice-D.pdf] .

Other issues to Consider

Government guidance and requirements will also require practices to reconsider other aspects of their compliance, including training. Training may be deliverable remotely or via digital means (e.g. via webinar) and you should consider what adaptations your practice can make to ensure compliance while staff are working remotely.

You should consider whether your policies, controls and procedures remain appropriate and whether they need adjustment to reflect what you or your practice is doing. If your CDD or EDD processes change then you should consider updating your Practice-Wide Risk Assessment, any matter risk assessment, and relevant policies.

If staff are working away from the office, you should ensure they have access to the necessary CDD documentation to be able to consider the risks of any client or matter.

If you are using digital video or photography to support your CDD, or obtaining other personal information, you should obtain consent from the data subject for the capture and storage of this information and have due regard to data protection requirements.

If you are requesting that personal or sensitive information be sent by email or other electronic means in support of CDD, due consideration should be made to the associated information security risks. You should consider and record the necessary steps to mitigate such risks (e.g. encryption).

If you have questions about whether a specific ID&V method is allowable or any other aspect

of the above, contact your supervisor. If necessary, obtain independent legal advice from an experienced legal practitioner.

It is not for your supervisor to provide specific legal advice and/or confirmation on the application of the MLRs. You are required to satisfy yourself on your legal/regulatory obligations under the MLRs and that you have complied with them.

While care has been taken to ensure that this Advisory Note is accurate, up to date and useful, members of the LSAG will not accept any legal liability in relation to this Advisory Note (which has not been HM Treasury approved).