

Best Practice Guide to the Key Issues

AML Spring Update 2023

INDEX

- 1** OVERVIEW - THE NEW REQUIREMENTS
- 2** SRA THEMATIC REPORT ON MLCO AND MLRO ROLES
- 6** INDEPENDENT AML AUDITS
- 10** RISK ASSESSMENT KEY POINTS
- 13** TECHNOLOGY
- 15** CRYPTO CURRENCY DEVELOPMENTS
- 19** CONCLUSION
- 20** YOUR KEY QUESTIONS ANSWERED
- 25** RISK & COMPLIANCE SERVICES



Overview

UK businesses should be aware of the changes to the 2017 Money Laundering Regulations (MLRs) that required further compliance requirements for in-scope firms. and that took effect in 2022.

The 2022 Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations, effective from 1 April 2023, will require businesses subject to the MLRs to conduct checks of the register of overseas entities (ROE) at Companies House for dealings with corporate entities.

For dealings with trust entities, businesses subject to the MLRs will have to comply with checks of the trust registration service (TRS) maintained by HM Revenue and Customs (HMRC).

These changes are intended to improve transparency and combat money laundering and terrorist financing, and failure to comply with these requirements could result in significant penalties for businesses. Legal experts are urging UK businesses to pay close attention to these changes and ensure that they are in compliance by the deadline to avoid potential legal and financial consequences.

TRUST SERVICES

Under the new Regulation 18C, it is prohibited for firms to provide trust services to individuals who are sanctioned. Furthermore, firms and members are not allowed to offer trust services to individuals connected with Russia, unless the services are part of an ongoing arrangement that was established before 16 December 2022.

This regulation is aimed at preventing money laundering and other financial crimes that may be facilitated through the use of trust services. Firms and members are advised to carefully review their compliance programs and ensure that they are in compliance with these new requirements to avoid potential legal and financial consequences.

REGISTER OF OVERSEAS ENTITIES REGULATIONS

Amendments that came into force in January 2023 aim to address the practical difficulties of verifying a person's status as a beneficial owner. The changes mean that certain information will no longer need to be verified, including information about a government or public authority who is a registrable beneficial owner (except their "status" as a beneficial owner and whether they are on the sanctions list), and information about the beneficiaries of a pension scheme trust.

Previously verified information does not need to be verified again when an overseas entity submits an update or applies for removal.

Section 1:

SRA Thematic Report on MLCO and MLRO roles

SRA THEMATIC REPORT ON MLCO AND MLRO ROLES

The SRA is the largest regulator of legal services in England and Wales, overseeing over 158,000 solicitors in 10,000 law firms. This also includes 6,500 firms who are supervised for Anti-Money Laundering (AML) requirements.

In 2021, it contacted over 50 firms to learn more about how the roles of a Money Laundering Compliance Officer (MLCO) and Money Laundering Reporting Officer (MLRO) worked in those firms. A detailed report was published by the regulator in November of the same year highlighting three main pillars of success that all MLCOs and MLROs should consider:

Authority

- The ability to command respect, make decisions, and stick to those decisions through to completion.
- The ability to access and use all information possessed by the firm.

Independence

- A focus on the firm's legal obligations rather than the short-term gain.
- The ability to make decisions without the influence of clients or other fee earners.

Resources

- To be given the time and space to consider the best course of action.
- To have provision, where possible, for a deputy to cover for them and supportive colleagues.

The MLCO must be a member of the Board or any equivalent Senior Management Body responsible for the strategy and direction of the organisation.

- A MLCO can delegate some of their duties to their MLRO. However, the MLCO will remain responsible for compliance and the point of contact for the SRA on AML.
- The MLRO's primary duty remains to submit suspicious activity reports (SARs) to the National Crime Agency (NCA); they carry personal liability for fulfilling this role.

Over 50 firms were contacted in 2021 by the SRA about the role of an MLRO/MLCO



A compliance regime can only be effective when all employees are engaged with the processes and procedures that are required to support good risk management.

KEY FINDINGS:

Generally, AML officers fulfil the two pillars of authority and independence well. They are able to command the respect of peers and are capable of making clear-sighted and risk-based decisions.

Their biggest challenge was resourcing, most acutely in relation to time:

- Time to learn about the role,
- Time to plan,
- Time to check the firm's progress,
- Time to reflect, and
- Time to act in an emergency.

All are significant parts of the role and need an appropriate investment.

If the MLCO or MLRO don't have enough time to dedicate to their duties, all other strategies – support, funding, training and so forth – are likely to be of limited use.

OTHER KEY FINDINGS

90% of firms who were approached had appointed the same person for both roles, which may not be appropriate. The SRA asked those firms in their sample that did the opposite, why they chose to have separate role holders. They gave different reasons, but can be summarised as:

- a fairer division of the work
- separating the compliance function from the firm's senior management
- a feeling that the role of MLCO sat naturally alongside that of Compliance Officer for Legal Practice (COLP)
- increasing the number of people fee earners could approach with any issues.

R18 PWRA should be compiled with team input and shared with others in the firm for transparency. The PWRA should be a living document that underpins the firm's AML regime, be shared with colleagues to enable them to understand the rationale for mitigation and reviewed whenever there are:

- changes to the services provided,
- legislation or associated announcements such as in high risk countries and sanctions,
- supervisory AML authority updates,
- changes to client base or delivery channels such as a move to remote working as a result of Covid-19.

Periodic reviews are also sensible. More use could be made of the PWRA, for example in training or explaining the underpinnings of the firm's AML Policy, Controls and Procedures (PCPs). It is very likely that the PWRA will have detail included which helps to explain why the firm adopts a certain approach to risk assessment that isn't necessarily appropriate for inclusion in the PCPs without lengthening what often can be already cumbersome documents.

MLROs should actively test their firm's AML regime to check how resilient their systems are.

- Independent file reviews are an acknowledged barometer of front line performance to your Policies Controls and Procedures (PCPs). Consequently, adding to the time required of an MLRO is an expectation that they will be completing their own independent file reviews to check:
 - staff are following AML requirements,
 - that EID searches are delivering to the standards required
 - staff are using the EID output data correctly, and
 - overall understanding of their staffs' AML training, whilst one to one feedback from file reviews generates greater awareness amongst staff for having PCPs in place, and more likely to identify other criminal activity, such as fraud.

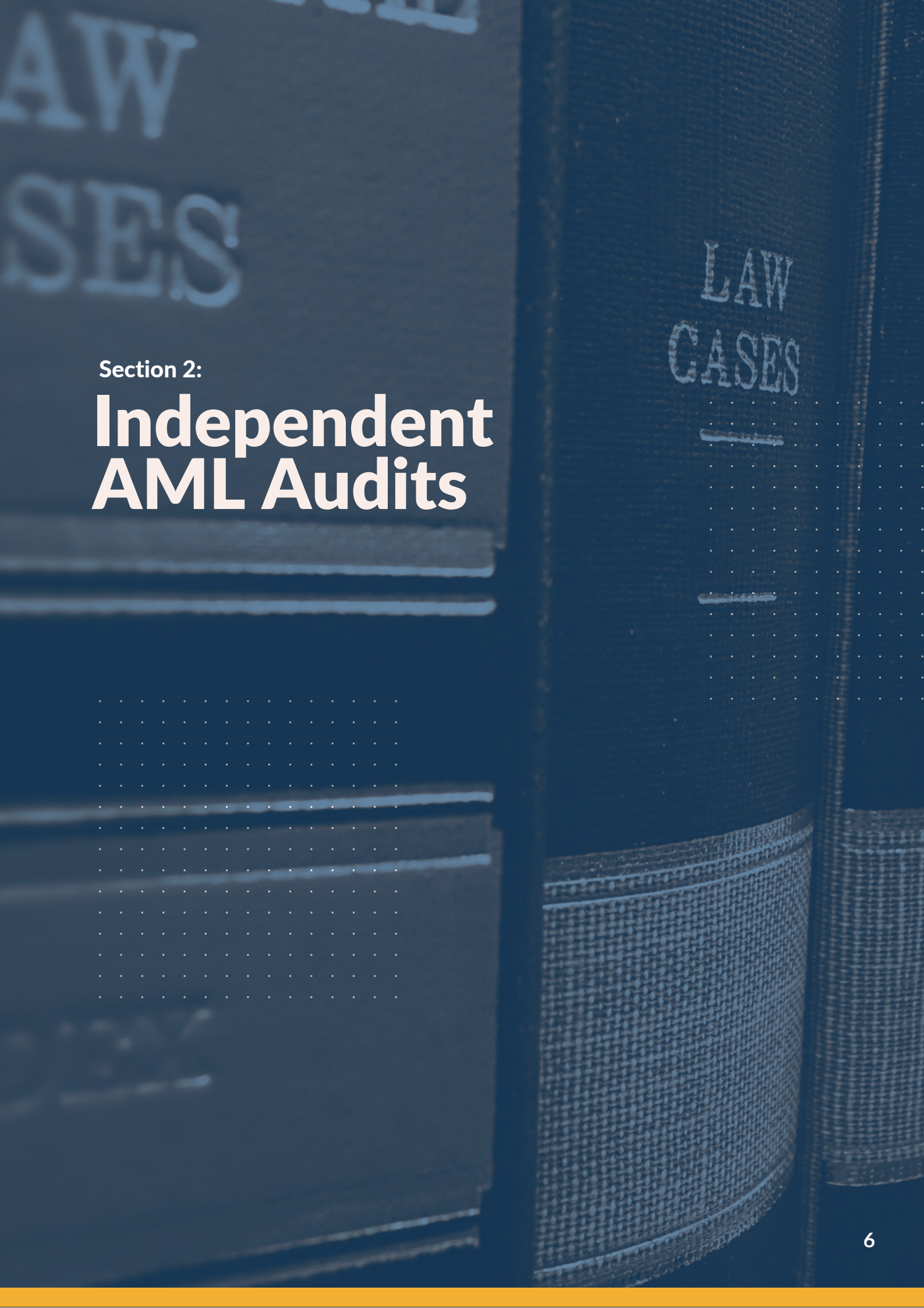
These are just some of the expectations that regulators will have, together with the follow-up activity where results are found wanting.

- Firms can help AML officers discharge their duties by limiting the number of additional roles they hold, reducing their fee-earning targets, and appointing dedicated staff to share the burden after securing approval.

Evidencing your findings is key to help your MLRO

Did you know about our

Policy & Procedure Store
[Find out more](#)



Section 2:

Independent AML Audits

KEY FINDINGS:

Legal Eye carried out a number of Independent AML audits over the course of 2022 and some of the most common themes the team have come across throughout are continuing into 2023.

The purpose of an independent audit function is to examine, evaluate and make recommendations regarding the adequacy and effectiveness of the practice's anti-money laundering and counter-terrorist financing policies, controls, and procedures (PCPs).

As per LSAG Guidance, the audit function must be independent of the function being reviewed, but it is not mandatory for the auditor to be external to the practice. Our team considers several factors to determine the best option for each client, whether internal or external.

Uppermost in your considerations must be that they - whether internal or external - have the requisite skills and knowledge in audit and AML/TF in order to be able to adequately carry out their duties.

Will they have the required time to invest in a thorough review and the necessary unfettered independence to report things as they are without fear or favour?

Outsourcing this service appears to be becoming a favoured route.



KEY FINDINGS:

- Top of the list for many MLROs are concerns that despite all the training and awareness given, worries remain that their staff may not fully understand what they should be doing and red flags may go unnoticed.
- The absence of a written or evidential client and matter risk assessment. They are a requirement, the absence of which will draw criticism from any regulator. Key, is that they are written down and demonstrate thought and not simply ticking boxes. Remember at college when you were told examiners will award marks for showing your workings out, even if you get the wrong answer. The same applies here, briefly noting your thoughts and reasons for being satisfied may save you at a later date when facing an investigation and struggling to recollect past events!.
- Many MLROs are overburdened with other roles and responsibilities that hinder their ability to understand the implications in other departments of the broader requirements of tax advice, or trust and company service provision, identify who might require separate AML officer authorisation as a beneficial Owner, Owner or Manager (BOOMs) and to review and keep updated Policies, Controls and procedures that are reflective of changing risks.
- Ongoing Staff screening requirements are not always evident or formalised as to what needs to be done and considered.
- Finally, awareness that Customer Due Diligence (CDD) material is to be kept in accordance with Money Laundering Regulation 40 for a minimum of 5 years and no longer than 10 without client consent, or notice of legal action is often not realised or disclosed. As for the firm's compliance, this is equally hard with, for example, ID held on individual matter files, which themselves may be archived for 15 years, or longer. Even where the firm has electronic separation in their case management system for this purpose, it is often not followed.

CDD material must be kept for a minimum of 5 years and no longer than 10

Did you
know about
our

**AML Independent Audit
including Certification**
[Find out more](#)

EVALUATION

Are you an MLRO and have sleepless nights worrying that staff might not follow or understand some of the firm's key AML Procedures despite their recent training? Can you safely say all your staff are doing what should be done when it comes to ID and risk assessment?

Revised guidance suggests AML training is conducted at least annually and that training has to be reflective of the AML risks associated with their role and in between those annual refreshers, staff training is risk based. That means, as you identify further AML issues perhaps from file reviews, statute, regulations, or your PCPs change, you develop a new service or delivery channel, this may trigger further training requirements. At the same time, training records are often not kept up to date, evidence of training being adequate, or reflecting risks, or considering what the firm has applied through its PCPs.

All of the above can be summarised into one word "Evaluation". As you know, evaluation is the process of considering if:

- key messages have been absorbed,
- if PCPs and individuals are performing as you want them to.

However, despite the concerns, often there is little evidence of any Evaluation taking place, either before, during or after the training has taken place. A thorough debrief after training to ensure MLCO, MLRO and staff are on the same page might consider:

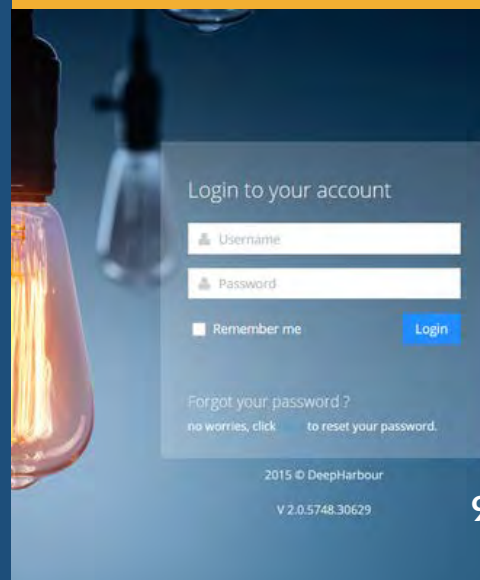
- What they have learnt from the training: how does that compare to your key messages and objectives?
- What are they going to do differently as a consequence of the training?
- What performance measures might we need to agree to ensure learnings are applied?
- What didn't they understand?
- What additional training or support might be appropriate?
- When should we next review this?



Did you know about our

Online Risk & Compliance Training System

[Find out more about The Legal Eye Academy.](#)




Section 3:

Risk Assessment Key Points

The following are some key risk assessment points to note:

- The risk assessment must be completed thoroughly on each occasion to demonstrate to a regulator a robust approach to due diligence. To ensure the assessment is not a tick-box process, at the end you summarise your overall reasons for the risk assessment of low, medium or high and any additional mitigation to be employed. The assessment is your explanation as to why in, for example, conveyancing where your AML risk starting point is 'High Risk' you judge this client and matter to be 'low risk'.
- At a simplified level, a written assessment template is a simple checklist of what to consider.
- The approach, you use in completing an assessment has to be capable of meeting the requirements of guidance, capable of demonstrating a robust approach to risk assessment across each file and driving your underlying due diligence.
- You must return at appropriate points in the transaction to update the assessment as new information comes to light and you must still be alert to any subsequent information that might raise suspicions or concerns. In conveyancing, for example,
 - when the mortgage offer is received, and source of wealth / funds can be confirmed.
 - perhaps again at pre-exchange, when the whole file can be reassessed ahead of client funds arriving in your client account.



**Did you
know about
our**

**Annual Risk
Assessment Service**

This independent assessment from Legal Eye helps you to benchmark your systems, policies and processes against peers and to devise a roadmap for future developments.

[Find out more](#)


KEY FINDINGS:

- A template form must never stop your professional judgement to assess a matter as high risk, despite template answers suggesting lower risk. Nor should it be used as a scorecard where 12 low answers outweigh one high risk answer – the opposite might apply!!
- Remember, the Regulations set out when you must take specific due diligence steps, notably EDD. For example, when dealing with PEPs and KCAs, or either of the parties to a transaction are established in a HRTC, and in the case of sanctions obtaining a licence from the Office of Financial Sanctions Implementation (OFSI).
- You must reflect the risks identified and document them into the Client and Matter Risk Assessment together with steps to mitigate those risks and you must be able to demonstrate to a Regulator CDD measures are appropriate in mitigation by recording reasons and actions into the risk assessment.



Section 4:

Technology



Technology continues to play a crucial role in AML developments, most notably via Electronic ID and Verification (EID & V). However, these are tools to aid your assessment, and of themselves do not eliminate risk completely. Other technologies include those aiding client onboarding, open-source banking, and facial recognition.

This allows data to be presented more easily to speed up and improve the process. However, you still need to recognise that whichever systems you choose, you need to complete a Technology Impact Assessment that considers whether your system is:

- secure from fraud,
- not open to misuse,
- capable of providing reasonable assurance that the person claiming the identity, is that person, and
- the limitations of the system.

In the case, of EID, other considerations are who can override a 'refer' or 'fail' and what additional actions are required dependent upon the nature of the alert. For example, we see alerts flagging a possible PEP, at which point staff will ask for certified ID, but that alone will not prove, or disprove PEP status. An EID search may not reveal a Known Close Associate, so you must still be alert to other information that may arise suggesting a PEP connection such as the Source of Funds checks. It's therefore important that thought is given to the EID outcome and how it should be managed. Even a straightforward pass decision may not be all that it seems. We have seen recent examples where the photo selfie was a photograph of the individual and the system passed the facial recognition test.

In another, the proof of address was a photo image of an Amazon Parcel Address label, which the system again accepted, albeit not in accordance with the list of acceptable ID used by the firm. Uploading passports is also another favourite where the client inadvertently obscures or misses the signature page of the new passport. Without a signature you may have a problem as a conveyancer complying with CML Handbook requirements on checking signatures. So it is important to review all of the data in the output report looking for anything that might require further attention. Remember these are tools to assist and not the definitive assurance some might give to them.

CRYPTOCURRENCIES DEVELOPMENTS

10th January 2023 marked 3 years of inclusion of crypto asset exchange providers and custodian wallet providers in scope for the UK Money Laundering Regulations (“MLRs”). It’s important to note that this definition encapsulates only a portion of the crypto sector, and there remain multiple facets of the crypto universe which sit outside of the regulatory perimeter.

In the EU, 6MLD introduced in late 2020, requires Enhanced Due Diligence for cryptocurrencies and the US is tightening its regulation. Here in the UK, we are not subject to 6MLD and regulators are still considering their positions, so there is no specific advice or framework, and the FCA now regulates all crypto exchanges in the UK.

Most cryptocurrencies are very volatile, if you have viewed the NCA warnings on Chinese Underground Banking, there are some parallels to be drawn with unofficial exchanges established by criminals to fund and process payments for their operations.

Useful guidance is provided in an [answer published on the Law Society of Scotland website](#) last year, which urges caution, and if you proceed, to make copious notes of your Enhanced Due Diligence.

The use of crypto may be indicative of higher risk

Guidance to Enhance Crypto AML Monitoring

The LSos Q&A guidance can be summarised into this starting point:

There are no reasons why you shouldn’t engage with clients wanting to use funds from their dealings in cryptocurrency. However, the use of crypto may be indicative of higher risk (as per LSAG Guidance s 5.6.1.3). Regulators and MLROs/MLCOs need to consider Enhanced Due Diligence to consider and document the factors you have taken into consideration regarding your risk assessment and the due diligence performed around the value of the crypto deposit and its source. Moreover, there is no one-size-fits all when it comes to diligence for crypto currency, so you need to take time to consider and document all available evidence, before deciding whether you should proceed with the matter.



Section 5:

The Ongoing Sanctions Regime

SANCTIONS

The UK sanctions regime introduced in 2022 applies to persons and entities where the UK government has:

- imposed sanctions unilaterally
- implemented sanctions imposed by the United Nations (UN) and as impending legislation is approved, on the back of EU and US sanctions.

The Sanctions and Anti-Money Laundering Act 2018 provides the main legal basis for the UK to impose, update and lift sanctions.

The law restricts you from:

- receiving payment from or making funds available to persons on the sanctions list
- dealing with their economic resources
- making even legitimate payments to those persons, including for you to receive reasonable fees for the provision of legal advice or services. OFSI will also judge whether the fees are reasonable when granting a licence to you.

These events are a trigger for you to review your firm's R18 AML risk assessment. You should consider how likely it is that your clients may be on the sanctions lists.

Although, the trigger here is the increased number of sanctions being applied to Russia and individuals from Russia, it's also worth remembering that even before current events started, it's been difficult to categorise the clients that may need to be checked simply by their nationality, or country of residence.

Just how likely is it your client is on the sanctions list?



UK nationals and UK residents can be on sanctions lists, so you may still be at risk even if you only act for local clients. There is also much talk of government ramping up the use of Unexplained Wealth Orders as another means to flush out dirty money in the UK. These also generally come with asset freezes attached to underlying assets whilst the recipient tries to explain how they got their funds to acquire the assets in question.

You also should remember that you cannot limit your risk assessment to the work regulated under the Money Laundering Regulations. Examples of unregulated work that sanctions may affect include:

- payment of personal injuries settlements
- property settlements following a divorce.

You'd also need a licence from OFSI to use legal aid payments for the benefit of a person on the sanctions list.

If you have a high risk of dealing with clients on the sanctions list, you should also have processes in place to help you find out whether key beneficial owners, or the intended recipient of funds from a transaction you're undertaking, are subject to the restrictions.

Remember, EID checks are usually using the latest lists at the time of the search, but this is a very fast-moving situation with frequent updates.

With this in mind, how often are your EID providers refreshing sanctions data? For ongoing relationships, you may need to search again, unless your EID package provides a change monitoring service – but for how long does that Watch List monitoring service last? Individuals can be added to the sanctions list after you have searched.

So, do you have a Sanctions Policy in place?

- For many, its embedded in your AML Policy – I know ours is in our precedent document. Is it current?
- Do staff know how to proceed if they receive a Sanctions alert in their EID check?

Your EID checks should be helping you to identify those sanctioned.

- Revisit EID risk assessment or guidance to ensure your EID checks are running a check in the background, especially where you are using a tiered EID system where the Simplified level perhaps does, or doesn't check?
- Do staff know which tiers to use and when?
- Does this need updating e.g. refresher training needed?
- Do you EID check ALL clients?

Where you receive a “refer” or “alert” in your EID checks, are you recording your reasons for over-riding and proceeding?

This is how you demonstrate to a Supervisor, you are actively engaged with AML and Sanctions Risks.

[The Law Society have updated their Guidance Note on Sanctions – it's a useful short read and reference point, whilst the SRA issued an update on 4th March.](#)

CONCLUSION

Money laundering remains a major concern for the legal industry in 2023, as headlines about illicit funds continue around Russian Elites, Proxies and Oligarchs (REPO). The UK government's efforts continue to work against these forces.

Additionally, reports of lawyers who have facilitated money laundering serve as a reminder that AML compliance is a top priority for law firms, regardless of their location.

As a result, it is critical for lawyers and law firms to ensure that their AML processes are up-to-date and effective. With the public and regulators scrutinising the legal profession more closely than ever before, law firms must remain vigilant and thoroughly evaluate their clients' compliance to avoid any issues with money laundering.

Legal Eye prides itself on offering straightforward, practical advice in a complicated compliance arena.

Get in touch today

 www.legal-eye.co.uk

 bestpractice@legal-eye.co.uk

 020 3051 2049

Connect with us



Your Key Questions Answered

Q: If acting for a buyer of a property, do we need to check the seller is not on a sanctions list before we send the money to them, or is that a matter for the seller's solicitor?

A: We believe, this would generally be for the seller's solicitor to address, in the same way that if there was a property fraud perpetrated by a bogus seller, it would fall at the door of the seller's solicitor. That said, you would need to be careful to not be on notice of anything untoward, as this might then attach some liability to you.

Q: Can a firm have more than one MLRO?

A: Yes, you can have as many MLROs as you want. However, in accordance with Section 4.7 of the LSAG Guidance, each will automatically be a manager and must therefore be approved as a BOOM (R26) prior to their appointment. If you are using a rotating model, you should consider all the individuals among whom the role is rotating as BOOMs and get them approved as such.

If you are operating a rotating model of MLROs among more than one person, the requirement to inform your supervisor within 14 days must be met whenever a new person takes over the lead position.

Q: Sanction say Russians can only hold £50,000 in a UK bank savings account. Is it safe to send proceeds of a sale to a UK current account held by Russians?

A: The UK government did announce plans for any funds over and above £50,000 to be frozen in the UK bank accounts of Russian citizens. We are not clear on whether legislation is now in place for this, so you will need to make further enquiries to establish more details. As a consequence, you should also be mindful of handling the sale of property or assets in Russian ownership and especially for those specifically named in sanctions lists. This is a very fast-moving situation and you should be directing this question to the [Office of Financial Sanctions Implementation \(OFSI\)](#) for further guidance.

Q: What does 'TCSP' stand for?

A: Trust and Company Service Provider. The SRA published a report in November 2020, which was subsequently updated in March 2021, requiring SRA firms to register with them if they are providing any of the following services:

1. forming companies or other legal persons;
2. acting, or arranging for another person to act:
 - a. as a director or secretary of a company
 - b. as a partner of a partnership
 - c. in a similar capacity in relation to other legal persons
3. providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or legal arrangement
4. acting, or arranging for another person to act, as:
 - d. trustee of an express trust or similar legal arrangement
 - e. a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

Q: Am I right in thinking that the JMLSG Guidance means that whoever maintains our client account is entitled to ask us to provide evidence of our CDD on any, or all of our clients? This is on the basis that as it is a 'pooled client account'. The bank or whoever maintains the client account is exempted from the requirement to do CDD which would otherwise apply to the bank in respect of a beneficial owner of a bank account. This is similar to anyone else who relies on our CDD in accordance with Regulation 39?

A: Yes, this is correct. In practice, we are not aware that banks are doing so, although in 2020/21 we did hear rumours that a small number of enquiries had started to emerge, but nothing widespread. We did not see any of the enquiries, so are unable to comment on any relationship to Regulation 39. However, it does stress the need to be meticulous in your ID, verification and due diligence. It would be very embarrassing for a firm's bank to raise issues over the quality or standard of due diligence conducted by the firm!



Q: If so, do we need to record this somewhere either in the AML documents we send to the client for the purpose of CDD or in our terms of business or engagement letter? If so, do you have any suitable wording we can use?

A: Yes, you need to include wording that discloses this to the client and it needs to be added to either your Terms of Business, Client Care Letter or other documents (or all of them) used to collect due diligence material. It is a legal obligation on Firms and Banks to actively comply with Money Laundering Regulations of which this forms part, so the client must be made aware of the use of their personal information on this way. As to wording, we suggest:

“The anti-money laundering guidance which UK banks and other financial services firms must adhere to is issued by the Joint Money Laundering Steering Group (‘JMLSG’). The JMLSG considers all clients with funds deposited in a law firm’s pooled client account to be beneficial owners of that account.

The JMLSG does not require banks to routinely identify the beneficial owners of law firm’s pooled accounts, as they do with most other accounts they issue. Pooled client accounts are granted this exemption on the proviso that this information is available upon request. In the event of our bank requesting information about the beneficial owners of our pooled client account, we have a legal obligation to disclose any information we have gathered as part of our client due diligence to them.”



Q: For firms falling outside the scope of AML, e.g. litigation only, we understand it is still necessary to conduct the AML R18 firm-wide risk assessment as well as AML training. However, CDD is not technically required to the same level as those firms operating within scope, is that all correct?

A: Your starting points are:

The Money Laundering Regulations 2017 which apply to Independent Legal Professionals and Trust or Company Service Providers defined as a firm or sole practitioner who by way of business provides legal or notarial services to other persons when participating in financial or real property transactions concerning:

- (a) the buying and selling of real property or business entities;
- (b) the managing of client money, securities or other assets;
- (c) the opening or management of bank, savings or securities accounts;
- (d) the organisation of contributions necessary for the creation, operation or management of companies; or
- (e) the creation, operation or management of trusts, companies, foundations or similar structures, and, for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

I've underlined the key points in the definition, which might bring your litigation work in scope of the MLRs.

- You should remember that the National AML Risk Assessment, together with the subsequent SRA AML Risk Assessment highlight the emerging risks of Sham Litigation (fake lawsuits between collaborating parties to launder money as the payment of damages through the courts).
- Although your work may initially be out of the scope of the MLRs, you must have due regard to anything which might create an offence under the Terrorism Act, Proceeds of Crime Act, Criminal Finances Act, PEP or Sanctions Regimes or if your work takes you into the realms of providing Tax Advice. These would automatically bring work into the scope of the MLRs.

Remember, POCA has far-reaching implications with the proceeds from any criminal activity no matter how menial and where you have grounds for suspecting or should have had reasonable grounds for suspicion you must consider a SAR. Any criminal activity widens out the impact into Fraud, Tax Evasion, Benefit Fraud, Environmental Crime, Cyber Crime, etc. Legal Professional Privilege could have an influence in how you deal with these situations, but initially its about identification of potential AML risk within the work that you do.

Acting for a PEP, their close associates or someone on the sanctions list is also an identifiable risk that must be appropriately addressed and applies irrespective of whether your litigation work is within the scope of the MLRs.

Likewise, anything other than providing relevant tax thresholds could be caught under the broader definition of tax advice. So, if during the settlement of a litigation claim you become involved in negotiating, structuring or advising on how best to receive a financial settlement.

For these reasons, it is appropriate to complete a comprehensive R18 Practice Wide Risk Assessment identifying and assessing all the money laundering and terrorist financing risks your practice faces. In doing so, you can demonstrate which areas of your work are generally out of scope and those areas that might fall in scope, or where PEPs and their Known Close Associates, Criminal Finances Act and Sanctions regimes may bring work into scope, together with your mitigation of risk.

You can then justify the level of AML training considered appropriate in such circumstances, remembering that such training must be provided appropriate to the risks identified and at least annually, unless risks emerge, which means more training should be provided.

In terms of due diligence, this is always driven by your client and matter risk assessment. When work is in-scope of the MLRs a more in-depth level of risk assessment and due diligence is required. That will mean if your litigation work initially is out of scope, but subsequently comes within scope, then you will have to consider if you need to conduct more due diligence appropriate to the risk identified – sometimes referred to as AML grade due diligence with greater emphasis on understanding beneficial ownership, client funds and wealth.

The answers given cannot be regarded as a definitive statement of the law or of the effect of the law, and do not comprise, and should not be relied on as giving, legal advice. They are prepared in good faith, but neither Legal Eye nor any of the individuals responsible for or involved in its preparation accept any legal responsibility or liability for anything done in reliance on these statements.

Legal Eye prides itself on offering straightforward, practical advice in a complicated compliance arena.

Get in touch today

 bestpractice@legal-eye.co.uk

 020 3051 2049

Policy & Procedure Store

A library of policies, precedents and helpful documents you'll need to create or add to a robust risk management framework for your firm.

[Find out more >](#)

Merger & Acquisition

Demonstrating that your business is well-run, efficient and prudently-managed with a strong risk framework in place can really help to achieve a successful outcome at this critical time in the journey of your practice.

[Find out more >](#)

Online Compliance Training

The Legal Eye Academy offers online training modules that cover the latest emerging risk and compliance issues and are continually updated to reflect changes in regulation.

[Find out more >](#)

AML Audit & Certification

An independent AML audit is now required by law firm regulators. Demonstrate your commitment to compliance and get started today.

[Find out more >](#)

Risk & Compliance Gap Analysis

With internal resources stretched like never before, have you ever considered having an independent firm wide review of your risk and compliance obligations?

[Find out more >](#)

CQS Gap Analysis

Are you ready for the changes to the CQS's Core Practice Management Standards (CPMS)? Legal Eye are now offering firms a gap analysis and CQS Accreditation Application Support.

[Find out more >](#)

Get in touch today

 www.legal-eye.co.uk

 bestpractice@legal-eye.co.uk

 020 3051 2049

Connect with us

