CLC AML Sector Risk Assessment

The CLC is obliged, under Regulation 17 of the 2017 AML Regulations, to conduct a risk assessment of its own sector regarding the international and domestic risks of money laundering and terrorist financing. This risk assessment sets out the main money laundering risks that we consider relevant to those we supervise and is a central tool in fulfilling the CLC's obligations under the new Economic Crime and Corporate Transparency Act (ECCTA) which introduced a new objective for legal regulators into the Legal Services Act 2007 to promote the prevention and detection of economic crime.

Money laundering is the process of concealing the origin, ownership or destination of illegally or dishonestly obtained money by hiding it within legitimate economic activities in order to make it appear legal. The impact of money laundering is significant as it, "…underpins and enables most forms of organised crime, allowing crime groups to further their operations and conceal their assets"[1]. The latest National Strategic Assessment has stated that there could be hundreds of billions of pounds laundered through and within the UK or UK registered corporate structures annually[2].

Preventing money laundering can remove criminals' incentives to traffic weapons, trade drugs or engage in human trafficking, and helps to reduce corruption to create a better, safer society.

Conveyancing is a common method for disposing of or converting criminal proceeds due to criminals being able to launder large amounts of money in a single transaction. Probate services (including estate administration and related work) may also be utilised for money laundering purposes and other structures such as trusts and corporate entities could be used as vehicles to disguise assets derived from the proceeds of crime.

What is the CLC's role?

The CLC is responsible for the supervision of its regulated community's compliance with AML Regulations and the relevant CLC codes and standards. This AML risk assessment is updated as required to ensure it takes into account emerging risks and trends.

To comply with the legal obligations contained in the Proceeds of Crime Act 2002, the Terrorism Act 2000 and the 2017 AML Regulations[3] (as amended) (MLRs), CLC regulated persons should have regard to the specific requirements under the CLC anti-money laundering and combating terrorist financing code and guidance. CLC Practices should also make use of the resources in the CLC AML Toolkit, including the Treasury-approved Legal Sector Affinity Group AML Guidance.

Who needs to consider this risk assessment?

The MLRs place obligations on CLC Practices to take appropriate steps to identify and assess their risk of being used for money laundering or terrorist financing.

CLC Practices are required to carry out a written practice-wide risk assessment to identify and assess not only the risk of money laundering and terrorist financing but also to assess the risk of proliferation

[1] National Crime Agency website.
[2] NCA National Strategic Assessment of Serious and Organised Crime 2025, which can be found here.
[3] As amended by the MLRs 2019 (The Fifth Money Laundering Directive [5MLD])

financing[4]. The PWRA should be updated at least every year and also whenever significant developments occur (such as new AML legislation or a change in the practice's services being offered). The CLC has developed a template PWRA which practices are encouraged to use here.

When practices develop their own risk assessments, they must, under Regulation 18(2)(a), take into account the risks contained in this sector risk assessment, the National Risk Assessment and knowledge of their services, clients and service delivery. Please note that the new National Risk Assessment (NRA) was published in July 2025. This sectoral risk assessment has been fully updated in light of the new NRA.

Practices must also have written policies, controls and procedures that enable effective management, monitoring and mitigation of the risks that have been identified. Client and matter risk assessments are also necessary under the MLRs to understand the risk arising in each individual matter and determine the extent of client due diligence. The CLC has produced a template matter risk assessment which can be found here in the CLC AML Toolkit.

Risk-based approach

The MLRs require you to take a risk-based approach to detecting and preventing money laundering. This means focussing resources on the areas that are most at risk of money laundering and undertaking not only a practice wide risk assessment but also client and matter risk assessments as practices must, under Regulation 28(12), ensure that their due diligence measures, "…reflect…(ii) its assessment of the level of risk arising in any particular case.".

With respect to client/matter risk assessments CLC practices are expected to ensure that these risk assessments, which must be recorded, take into account relevant factors, reflect the findings of your practice wide risk assessment and come to a conclusion as to risk rating. The level of risk arising in any particular matter will determine what level of due diligence you undertake and it is recommended to conduct risk assessments not only at the outset at the transaction but also during the transaction as well – for example in response to significant developments such as a change in the client's source of funds.

The CLC takes a risk-based approach to supervision and targets resources at those practices considered to be higher risk which is informed by a variety of sources such as AML intelligence and previous AML compliance ratings. This risk assessment will also take into account emerging risks: new technologies (including cryptocurrency and the use of AI to circumvent CDD) and property developers.

Red flags/alerts

It is important to be aware of, and act properly upon, red flag indicators that a transaction may be suspicious. One red flag may provide a basis for making further enquiries of your client. Several red flag indicators together, without reasonable explanation, are more likely to provide grounds for suspicion.

You should consider which circumstances in your experience are unusual. If further enquiries do not satisfy your suspicions, you should refer the matter to your practice's Money Laundering Reporting Officer (MLRO) who will decide whether a Suspicious Activity Report (SAR) needs to be filed with the NCA.

The CLC published a consolidated list of updated red flags in conveyancing transactions in March 2025 which practices are strongly encouraged to read. This list is not intended to be a tick-list nor to be exhaustive but it may help you to consider which circumstances in your experience are unusual.

[4] This requirement was introduced by the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 which came into force on 1 April 2023.

National Risk Assessment 2025

The National Risk Assessment 2025 continues to assess professional services as a crucial gateway for criminals looking to disguise the origin of their funds. The report notes that legal services remain at **high risk**[5] of being abused by money launderers and suggests that high-end money laundering almost always requires facilitation by legal services, even if they are unwitting.

The new National Risk Assessment continues to assess the following services to be at a high risk of money laundering:

- Conveyancing[6]
- Misuse of client accounts[7]
- Trust and company service providers (TCSPs)[8]

To mitigate risks when providing services in these areas, you must make sure that you comply with the latest AML guidance and be aware of red flags that could cause you to have suspicions of money laundering.

Key changes for CLC practices in the 2025 NRA:

1. **Cryptoassets** have been upgraded from medium risk to high risk in the 2025 NRA. As cryptoassets are being increasingly used in conveyancing transactions (or at the least being proposed), the CLC would urge practices to be extremely cautious about accepting money that has originated in full or in part from cryptoassets. This risk assessment goes into detail on cryptoassets in the section on "emerging risks" below.
2. **Electronic Money Institutions/PSPs** have been assessed as being "high risk", increasing from medium risk in 2020. These organisations offer alternatives to traditional banking models by offering "non-bank payment services". The NRA states: "The rapid scaling of the sector since 2020, increased complexity and diversification of services, has contributed to the sector's attractiveness for criminals, with increased options to manage and launder funds cross border." (paragraph 5.64) Some examples of EMIs are: Revolut and Paypal.
3. **Sanctions evasion:** a growing "convergence" between sanctions evasion, money laundering and kleptocracy has been identified in the 2025 NRA. They identify that, "…Sanctioned entities and individuals aim to conceal the links to their funds by leveraging existing money laundering networks and using the same international controller networks, complicit professionals and complex structures that were previously principally used by those seeking to launder high volumes of criminal funds." (paragraph 3.3).
4. **Property developers:** The NRA 2025 identifies a number of unregulated sectors which are of concern

[5] National Risk Assessment 2025: Paragraph 5.193.

[6] The NRA states: "…It often involves legal service professionals who are essential for most property purchase[s] in the UK. The purchase of property in the UK is attractive to criminals who seek to launder large sums of illicit funds in a single transaction, both to disguise their wealth and to benefit from the use or ownership." (Paragraph 5.202)

[7] The NRA states: "…they can be misused by criminals to both move illicit funds and to provide a veil of legitimacy to the proceeds of crime." (paragraph 5.205)

[8] Some of the key messages in the NRA are: "…The use of complex structures and legal arrangements, use of virtual office addresses not connected to beneficial owners, and the combination of services involving intermediaries and nominees, can facilitate anonymity. This anonymity is attractive to criminals looking to distance the criminal origin of the funds." (paragraph 5.225)

and present a potential risk. The most relevant for CLC practices are property developers. As is noted in the NRA, developers need to fulfil certain criteria in order to fall within scope of the MLRs. A particular vulnerability identified in the NRA 2025 are overseas buyers purchasing "off plan" properties and there are issues with developers looking at and understanding source of funds. This area will be explored in more detail in the "emerging risks section" of this risk assessment.

RISK FACTORS

The different types of risk that we consider to be relevant for CLC Practices are:

Product/service (High Risk):

- Conveyancing

Conveyancing, both residential and commercial, is a common method for disposing of or converting criminal proceeds due to being able to launder large amounts of money in a single transaction. Properties can be used to launder money by posing as rental properties to 'wash' illegitimate funds by disguising it as rental income. Remember that criminals also need somewhere to live and carry out their illegal work. Criminals may also use illegitimate monies as large and early repayments on a mortgage. The emergence of sanctions evasion, as noted in the NRA 2025, and the attractiveness of the UK property market heightens the risk of conveyancing in the UK being exploited in order to disguise illicit funds.

- Client account

Lawyers' client accounts can be used as a way to make illegal monies seem to have a legitimate source. Client accounts must never be used as a banking facility, or to pass funds through without a legitimate underlying legal transaction. It is good practice to withhold details of your client account until the necessary client due diligence has been completed.

Product/service (Medium risk):

- Trusts and trust related services

The kind of work which CLC practices are involved in under this service include acting or arranging for someone else to act as a trustee in the administration of an estate and/or involvement in the creation and/or management of trusts. Offshore trusts have been typically considered as higher risk which remains the case in the NRA 2025. There is little evidence that UK trusts, by themselves, are used for money laundering and terrorist financing however the new NRA 2025 has identified that certain UK trusts may be considered to be a higher risk such as trusts used to hold UK property, discretionary trusts and interest in possession trusts.

The CLC undertook a thematic review in the area of TCSPs in 2023 and 2024 and concluded, due to weak controls which were identified in some of the practices that participated, that the risk was medium. We would like to emphasise that client/matter risk assessments are expected on all relevant trust matters which are in scope of the AML Regulations. With adequate controls in place the risk of trust and trust related services for CLC practices is likely to be low to medium risk.

Furthermore, trust assets need to be carefully scrutinised and understood by CLC practices and we would advise that in low to medium risk situations the practice should enquire with the client as to source of the funds (or the source of funds that were used to purchase the asset being placed into trust) and record this on file. In high-risk situations, practices should undertake further checking which may involve obtaining documentation relating to the source of funds such as bank statements or completion statements and ensuring that the client's source of wealth is understood. A comprehensive risk assessment of trusts can be found in the TCSP thematic review.

Product/service (Low Risk):

- Company Service Providers

Corporate structures which enable anonymity can help to disguise the source or destination of money or assets. Law enforcement has stated that many investigations of money laundering involve opaque corporate structures that are used to hide the beneficial owner of assets. This is often used together with other services (in particular the purchase of property) to facilitate money laundering.

The CLC's thematic review into TCSP's identified that CLC practices are rarely involved in company formation however some exceptions were identified: incorporating management companies in freehold developments or forming companies for leaseholders to purchase the freehold through collective enfranchisement.

The CLC's conclusion on both of these kinds of company formation was they were low risk as they were closely linked to property, are non-complex (do not offer anonymity) and set up for a very narrow specific purpose within the UK. The complete risk assessment can be found in the TCSP thematic review.

- Probate and estate administration

Although these services are not explicitly mentioned in the National Risk Assessment (NRA) the CLC recognises that they may still be exploited by money launderers. In particular estate administration involves large amounts of monies coming into regulated client accounts from a range of sources and then being paid out to beneficiaries. These monies are sometimes not checked with the same level of scrutiny as other transactions and there is a risk that they could be given the appearance of legitimacy by going through a practice's client account.

- Remortgage work

Although this service is closely linked with conveyancing, it is considered to represent a lesser risk of money laundering due to the fact that money is typically not required from the client. If there is a shortfall however, meaning that the amount the client is borrowing is not enough to repay the existing lender, then the client will be required to produce additional funds which may increase the risk.

Client risk factors

Each client is different which will be reflected in their individual risk-profiles. A one-size-fits all approach to risk assessment is unlikely to be an adequate way to discharge obligations under the MLRs. There are a number of factors that increase the risk of money laundering presented by clients and beneficial owners, if applicable.

- Politically Exposed Persons (PEPs)

PEPs, both overseas and domestic, are considered higher risk as they are susceptible to bribery and corruption by virtue of their position which brings them power, influence and access. PEPs and their close families and associates must be identified and enhanced due diligence checks are required to mitigate the risks of corruption. Recent legislative changes permit a lower form of EDD for domestic PEPs vs overseas PEPs which should be carefully considered.

- Clients seeking anonymity or who cannot prove their identity

Clients who seek anonymity on behalf of themselves, a third party or beneficial owner, may be seeking to launder money. In some circumstances a client might legitimately not be able to produce identification documents in which case further investigations should be made. Clients who are evasive about proving their identity or who produce non-standard documentation might be considered higher

risk if there is no good explanation for this.

- Duration and nature of client relationships

The CLC's supervisory experience has identified situations where practices have failed to undertake adequate client due diligence when there is a pre-existing business or personal relationship with the client. Assumptions which have been made about a client's source of funds in particular should be challenged robustly and practices must obtain evidence of source of funds in all situations especially when dealing with conveyancing, which is considered to be high risk in terms of AML.

Another relevant factor to consider is whether the practice undertakes high volume work with a high client turnover. This is often the case with conveyancing (as opposed to other boutique or specialist services) and can lead to a superficial understanding or a client's background - which could mean there is a greater inherent AML risk.

- Clients who are involved in high-risk businesses or industries

The LSAG Guidance lists a number of what are considered to be high-risk businesses due to their nature such as cash intensive businesses like taxi firms, restaurants, pubs, betting shops, vape shops and others. CLC practices can act for non-natural persons and also may encounter source of funds which are derived from such business activities. The nature of the business should always be taken into account by the practice and fully recognised within the client/matter risk assessment. A further risk factor may also be businesses in high risk sectors that don't have any customers.

- Corporate entities as clients

In this risk assessment the CLC is highlighting corporate clients as a significant risk for CLC practices. Companies can be used as vehicles for money laundering and are useful tools for criminals to disguise their identities and launder assets. Proper CDD on corporate clients is essential and this includes: ensuring that the beneficial owner is properly identified and verified, obtaining and verifying the name of the body corporate, its company number or other registration number, the address of its registered office and taking reasonable measures to understand the ownership and control structure of the company.

Particular care should also be taken when trying to understand and obtain evidence of the source of funds (SOF) and source of wealth (SOW)[9] for any transaction involving a corporate entity. Regulation 28 of the AML Regulations contains the precise obligations which we would encourage practices to read carefully[10].

The CLC has identified the following particular risk factors for corporate clients which CLC practices must take into account when conducting proper client due diligence[11]:

- Corporate clients who have a foreign company named as the Person with Significant Control (PSC). This is contrary to UK Company Law which requires that companies disclose the individuals who control it. The law is, in practice, ignored by certain companies so CLC practices should take care when they come across such situations. According to Tax Policy Associates research, as

[9] For resources relating to SOF/SOW we would encourage practices to visit our AML toolkit: https://www.clc-uk.org/lawyers/anti-money-laundering-toolkit/

[10] Regulations 28(3), (3A), (4), (5), (6), (7), (8), (9), (10) and 11(a) are all relevant to CDD for corporate clients.

[11] A number of these risk factors have been put together in light of the extensive work and research of Tax Policy Associates which is an independent tax think tank that, amongst other activities, alerts the public to concerns around fraudulent companies and potential tax issues. Their website can be found here.

many as 50,000 UK companies hide their beneficial ownership in this way[12]. Such conduct could be indicative of a company which intends to hide its beneficial owner.

- Dormant companies: although there is a legitimate basis for ensuring that companies that are "dormant", which for Companies House is defined as there having been no "significant" transactions in the financial year, do not need to file audited accounts, this is unfortunately open to abuse. CLC practices should take care that such companies are genuinely "dormant" and not a fraudulent enterprise that is attempting to conceal assets or profits from public scrutiny. Research has demonstrated that a number of potentially fraudulent companies use this technique. For example, this company has filed dormant accounts but recent reporting has suggested it doesn't exist.

- Fake banks: Specific permission is required from the Financial Conduct Authority (FCA) to include the word "bank" in a company name. This can be circumvented, however, by ensuring the company is categorised as a bank on Companies House which enables fraud. This is something that CLC practices should also be wary of when acting for such corporate clients. One way of checking this is to ensure that the "bank" that the practice is acting for is regulated by the FCA. The way to identify if a company has categorised itself as a bank is to look at the "Nature of Business" section on Companies House when obtaining information about the corporate client. In this example, Credit London Ltd, you can see the specific bank code (64191) at the bottom of the page on Companies House.

- Off the shelf companies: These are companies that have already been setup by Companies House, typically by a formation agent, and which are transferred to new owners who purchase them and inherit aspects such as a pre-established bank account and lines of credit. They can give the appearance of a legitimate company that has genuine operations. In some instances, this may be a method of deception and it is of note that the National Risk Assessment (NRA) 2025[13] highlights such companies as representing a money laundering risk and identifies that such companies may be used in "phoenixing" whereby criminals seek to continue their operations without the poor reputation of a prior company[14]. It is also of note that the Panama Papers highlighted the use of shelf companies by global elites to hide assets and avoid the payment of tax.

- Shell companies: These kinds of companies are a well-established money laundering risk and relate to companies that have no significant operations, employees, offices and/or assets themselves but maintain their legal status and a bank account that can be useful for obscuring ownership, holding or moving illegitimate funds. One of the case studies in the new NRA 2025 highlights the use and setup of shell companies by a Chinese national to obtain loans worth tens of billions of pounds which were then used to purchase and invest in property development in the UK[15]. Additional risk factors are shell companies set up in jurisdictions with minimal regulatory oversight such as tax havens or countries where secrecy of ownership is permitted.

- Other indicators of fraud: these include non-dormant companies that have failed to file their accounts as they should have, mail being sent to the corporate entities' registered office being

[12] https://taxpolicy.org.uk/2025/03/19/50000-uk-companies-fail-to-declare-their-beneficial-owner/
[13] See NRA 2025 at paragraphs 3.101 – 3.104.
[14] A tip to spot such companies is to look at how the company was formed on Companies House and it should be possible to identify that a company formation agent was involved. Long periods of inactivity should also be evident from the records and potentially questioned with the client. The use of nominee directors in such companies is also a particularly telling sign.
[15] See NRA 2025 at page 49 (Box 3.L).

returned or the registered office being in dispute. In the latter instance some companies "squat" at certain addresses which may be an indicator of fraud. CLC practices should also take care with recently established companies (such as companies set up specifically for the property transaction) and ensure that source of funds and source of wealth is carefully documented and scrutinised. A final indicator of fraud the CLC would wish to emphasise are companies with questionable or entirely fake directors (either completely fake individuals or people who are recruited often through social media to lend their names to companies they don't actually control).

The CLC would emphasise that particular care should be taken when trying to obtain and scrutinise source of funds and source of wealth for corporate clients. If a corporate client informs you that the funds for the transaction derive from business profits, CLC practices should undertake appropriate work to ensure that these profits are legitimate and not derived from illegitimate funds. Any evidence obtained (such as profit and loss accounts) should be recorded and retained on file.

Transaction

Practices should be aware of any circumstances about a transaction which appear to be unusual or do not make commercial sense. The use of cash in a transaction suggests a higher risk, and it is a good idea to have a policy on the amount of cash you will accept and in what circumstances.

- Size and value of transaction

Criminals may seek large or high value transactions to launder as much money as possible in one go. If there is no good explanation for an unusually large transaction, or a client is seeking to make a number of linked transactions this may present a higher risk.

- Payment type

Cash and some electronic currencies/cryptocurrencies[16] can enable anonymity and present significant challenges in tracing their source[17]. There may be legitimate reasons that a client wants to pay in cash or electronic currency, however this should be considered higher risk because it has not passed through the banking system and is often untraceable.

- Transactions that don't fit with the practice or client's normal pattern

If a new or existing client requests services that aren't usually offered by your practice, you might consider it suspicious if there is no obvious reason for the request.

- Services that facilitate anonymity

Practices should be alert to clients seeking services that enable anonymity and allow beneficial owners to remain hidden without a reasonable explanation.

- New services, delivery methods or technologies

Criminals might target practices moving into new areas, because of the perception that their AML policies and procedures are new and untested. Criminals might also seek to target loopholes in new technology before they are identified and protected.

- Complex transactions

[16] The National Risk Assessment 2025 identifies 'cryptoassets' as being at a high risk of being used for money laundering which is a notable increase from 2020.

[17] Practices should note that if client due diligence (which includes source of funds) cannot be concluded then the business relationship should be terminated under the AML Regulations. Practices should also note that some insurance providers may not extend PII cover to transactions involving cryptocurrency so practices should check the insurance position first.

Criminals can use complexity as a way of concealing the source of funds or their ownership. Practices should make sure that they fully understand the purpose and nature of a transaction.

- Red flag transactions

CLC practices should note that the Fifth Money Laundering Directive (5MLD) expanded the situations in which red flag transactions would obligate a practice or firm to undertake Enhanced Due Diligence (EDD). The changes mean that practices must apply EDD where:

- where the transaction is complex
- where the transaction is unusually large or
- where there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose (formerly both conditions had to be satisfied).

Whether a transaction is "complex" or "unusually large" should be considered in relation to the normal conveyancing/probate activity of the practice and also the normal activity of the client.

Previously EDD was necessary only where all of the above elements were satisfied and now only one element needs to be engaged for EDD to be necessary.

This broadens the scope of this particular section considerably and we would advise CLC practices to pay careful regard to this when undertaking matter risk assessments and considering the level of client due diligence to be applied.

- Proliferation financing (additional risk factor)

All CLC practices must ensure that the risk of proliferation financing is risk assessed as part of their PWRA after legislative changes in 2023. Proliferation financing relates to the act of providing funds or financial services for use in the "manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons."[18]

The CLC's view is that conveyancing services, as well as the full range of services which CLC practices offer, is at a low risk of being exposed to such funds however CLC practices are reminded to be wary of funds or clients (both natural and non-natural persons) which may have a link or connection to the weapons trade and be aware that some sectors, such as the insurance sector, shipping/maritime or military/defence, or clients established in countries subject to sanctions may represent an increased risk which should be considered carefully.

Delivery channel

- Remote clients

Not seeing a client face-to-face (or engaging with them only through intermediaries) increases the risk of identity fraud and may help facilitate anonymity. The risk posed by remote clients can be mitigated by the use of safeguards such as electronic signatures and e-verification. You should consider using an electronic identity system that provides you with an adequate level of assurance that the client is who they say they are. This is particularly important as remote working and transactions become more common. It should also be noted that 5MLD introduced additional high-risk factors (when considering whether to apply EDD) and one of them was "whether the firm

[18] LSAG Guidance: page 33

operates without face to face meeting and without electronic identity systems to mitigate this".

- Payments to or from third parties

Criminals may seek to disguise the source of funds by third parties making or receiving payments. This is a way of disguising assets and practices should make sure the source of funds and source of wealth are identified and verified with no gaps. There may be legitimate reasons for third party payments, for example parents gifting a house deposit to their child. You should ensure you carry out appropriate due diligence on the source of funds and wealth (and retain appropriate evidence on file as you would for a client) and the reason for the payment before accepting funds. CLC practices should only accept funds from third parties in exceptional circumstances.

Geographical

- Location of client and beneficial owners

If clients, beneficial owners or third parties are based outside of the UK, you should consider applying enhanced due diligence measures, especially if dealing with countries with significant levels of corruption or other criminal activity, such as terrorism. EDD is mandated for certain countries on the UK's list of high risk third countries which can be found on the FATF website (the "grey" and "black" lists). This list is updated at every FATF plenary meeting.

Emerging risks:

- Cryptocurrency as a funding method for transactions:

As noted in this sectoral risk assessment, the NRA 2025 has assessed the risk of money laundering from cryptoassets to be high risk, a notable increase from the NRA 2020. The reason for this upgrade is due to cryptoassets increasingly appearing in money laundering intelligence since the last NRA in 2020. The NRA states:

"Cryptoassets are increasingly used for laundering all forms of proceeds of crime. In addition, there have been increasing levels of cryptoassets obtained through illicit means such as cybercrime, ransomware and cryptoasset thefts which are then laundered."[19]

The NRA goes on to identify that although Bitcoin remains an attractive cryptoasset for "illicit finance and serious and organised crime (SOC)", other forms of cryptocurrency are becoming popular with criminals such as stablecoin. The example given by the NRA 2025 is Tether and it is noted that the price stability, "fast transaction speed and wide adoption" have been factors behind its use[20].

OPBAS, the AML Regulator of Professional Body Supervisors (PBSs) recently published a letter which advised of the inherent risks in conveyancing and highlighted: "We note an emergence of cryptoassets interacting with property transactions, including through tokenisation, with the potential to impact the future AML risk landscape."

Evidence quite clearly points to cryptoassets being a significant red flag for practices and the CLC would urge practices to be vigilant and exercise extreme caution in any transaction before accepting cryptocurrency which has been converted to more traditional currencies. This is a complex area involving very elaborate schemes which are difficult to trace, and which may lack transparency (particularly regarding the source of funds which is a crucial AML obligation).

[19] NRA 2025 at paragraph 3.61.
[20] Ibid.

The CLC is aware that increasing numbers of clients are looking to fund or partly fund property purchases using cryptocurrency. Caution should be exercised in such situations and it is strongly recommended that each practice ensures that their AML policy and procedure cover all potential scenarios to ensure consistency of approach. Consistent training should be provided to staff as well to further embed established procedures and to alert staff to the money laundering risks which are present.

Professional Indemnity Insurance (PII) providers may also be reluctant to extend insurance cover to transactions that cover cryptocurrency and care should be taken to establish the PII position first. If a practice decides to proceed with a transaction (either wholly or partly funded by funds that have derived from crypto) then it should take care to ensure that the source of funds (SOF) and source of wealth (SOW) of the transaction are firmly established and well documented. If a CLC practice cannot establish these two crucial aspects of CDD, then the transaction should be terminated and any suspicions reported appropriately to the National Crime Agency (NCA).

CLC practices should also bear in mind that a regulatory regime for cryptoassets is currently in place, regulated by the Financial Conduct Authority (FCA). CLC practices are able to search this register when considering different companies that offer crypto services which is an important risk factor to consider in such scenarios as an unregulated cryptocurrency providers present a higher money laundering risk. The FCA register can be accessed here: here

- Use of AI to circumvent CDD:

The CLC has not seen any recent examples of AI being used to circumvent CDD, however we are of the view that it must be highlighted as an emerging risk due to the rapid and developing nature of the technology as well as intelligence from other sectors. One reason behind this is that the NRA 2025 has introduced a section on "cross cutting" risks and has specifically highlighted the opportunities and also the threats that AI presents:

"Current use of AI for money laundering is not fully understood but is not currently believed to be widespread; however, engagement between the private sector and law enforcement suggests that there has been use of AI for synthetic bank account creation, fraud and impersonation, phishing and on-boarding of money mules.[21]"

The CLC has also noted that sectors such as casinos have seen attempts to bypass CDD with AI and consider it is only a matter of time before CLC practices will have to reckon with such attempts as the technology develops and becomes more widely available. In the NRA 2025 there is a specific paragraph on "identity theft and synthetic accounts" which we would strongly encourage CLC practices to read and consider. It states:

"…Generative AI could potentially help criminals to pass banks and other firms' onboarding checks by creating synthetic identities or generating images to match stolen documents that is required to pass those tests."

CLC practices should ensure that any electronic systems they use are sufficiently robust in order to combat AI being used to try and circumvent them. We would recommend that CLC practices contact their providers and seek to understand just how secure the systems that are being used are and whether mitigations are in place (such as human checks in the process). We would remind all who we regulate that this is a specific requirement under Paragraph 6 of the CLC's AML & CTF Code:

[21] NRA 2025 at paragraph 6.1.

"6. Any system or product you use must be sufficiently robust to provide the necessary degree of certainty and incorporate qualitative checks that assess the strength of information supplied…"

- Property developers:

The NRA 2025 has highlighted property developers as a sector which is potentially unregulated under the AML regulations. Whether a property developer falls under the AML Regulations is linked to the type of business structure they have: if the developer sells their own properties within the same legal entity they are not in scope but if the sales are made through a separate legal entity then the sales entity will fall within scope of the MLRs.

CLC practices should bear the above in mind when engaging with developers and when assessing the money laundering risks of transactions. As is noted in the NRA 2025, developers, "…buy land, obtain planning permission, build property and sell it to realise a profit."[22] In addition, they often receive client money such as holding deposits or pre-sales and can also contribute money towards the deposits of clients.

The NRA 2025 notes that as little as 26% of the developers operating in the UK are registered with HMRC as Estate Agents Business (EABs). Others may be registered with FCA due to financial services and would therefore be supervised for AML in this way. CLC practices should review the developers they are working with to establish whether they are supervised or not.

Another important point made in the NRA 2025 is that developers often engage with overseas buyers who frequently purchase "off plan" properties which are purchases made directly with developers. This presents issues with establishing source of funds and it is unclear the extent to which unregulated developers properly and robustly scrutinise source of funds in such transactions. The NRA 2025 presents a common scenario in which Chinese buyers purchase off-plan UK developments through British Virgin Islands (BVI) companies – it is not clear in such scenarios who would be responsible for CDD checks.

As noted in the CLC's 2024 AML report, the CLC has received intelligence which demonstrates that developers have been requesting that conveyancing practices provide undertakings to confirm that they have identified the individual who is acquiring the property and have performed appropriate CDD (including how the property was funded). We would reiterate the conclusion in the 2024 AML report:

"CLC practices should ensure that any undertakings given only relate to actions which the conveyancer can reasonably undertake in the normal course of conveyancing transactions. The undertakings should be reviewed carefully and a practice-wide policy implemented with appropriate training provided to staff.[23]"

Next steps/available resources

We will regularly review this risk assessment, taking into account new information from government, law enforcement and our regulatory regime.

This report should be considered when practices are developing their own risk assessments under Regulation 18(1) MLR 2017 along with the National Risk Assessment 2025 and knowledge of their services, clients and delivery channels.

You should also consider the descriptions of risks and mitigations in the HMT-approved Legal Sector

[22] NRA 2025 at paragraph 5.259.
[23] CLC AML report (2024) at page 35.

Affinity Group's AML Guidance when writing your own practice-wide risk assessment.

We review practices' written risk assessments as part of our routine monitoring and inspections, or in response to specific information we receive. If you have any questions please contact our dedicated AML inbox at: aml@clc-uk.org.

Last reviewed: 7 October 2025