CLC AML risk assessment

This risk assessment sets out the main money laundering risks that we consider relevant to those we supervise.

- Why is money laundering a risk?

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[1].

The impact of money laundering on the UK is significant. Previous figures of £36 billion to £90 billion for all money laundering impacting the UK[2] are said to be a considerable underestimation.

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. This is highlighted by the National Crime Agency (NCA) who suggest that in 2016, 50 per cent of legal sector Suspicious Activity Reports (SARs) were linked to property transactions.

- What is the CLC's role?

The CLC is responsible for the supervision of anti-money laundering (AML). We work to identify those who may willingly help money launderers, and inform and educate those who might be unwittingly used by criminals.

This is the first AML risk assessment we have published, and we will update it on a regular basis to ensure it contains emerging risks and trends.

To comply with the legal obligations contained in the Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), CLC regulated persons should have regard to the specific outcomes under the CLC Code of Conduct outcome 1(m) and the CLC anti-money laundering and combating terrorist financing code and guidance.

[1] http://www.transparency.org/glossary/term/money_laundering
[2] National Strategic Assessment 2017, National Crime Agency

Who does it apply to?

The MLR 2017 places 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 the risk of money laundering and terrorist financing. This should be updated at least every year.

When practices develop their own risk assessments, they should take into account the risks contained in this report, the National Risk Assessment and knowledge of their services, clients and service delivery. We have produced a summary of the areas of the National Risk Assessment that are most relevant to CLC Practices which you can find here.

Practices must also have written policies, controls and procedures that enable effective management, monitoring and mitigation of the risks that have been identified.

Risk-based approach

The risk-based approach is embedded in UK legislation and AML best practice. It means that firms should focus their resources on the areas that are most at risk of money laundering.

We take a risk-based approach in directing our resources to having the greatest supervision of practices that have a higher risk of being used to launder money. We review practices' written risk assessments as part of our routine monitoring and inspections, or in response to specific information we receive. We will take appropriate action where we find instances of non-compliance.

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 SAR needs to be filed with the NCA.

We have published two documents which give information on red flag indicators. The lists are not intended to be a tick-list nor to be exhaustive but they may help you to consider which circumstances in your experience are unusual.

The first document outlines some of the high level AML red flag indicators as identified by the Financial Action Taskforce (FATF). The second document provides more detailed warning signs that you may come across in conveyancing transactions.

National Risk Assessment 2017

The National Risk Assessment 2017 states that professional services are a crucial gateway for criminals looking to disguise the origin of their funds. The report notes that legal services, like banking and accountancy services, remain at high risk 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 identification of a sector as 'high risk' means that those working in that sector *'should be vigilant towards the persistent efforts of criminals and terrorists to exploit…vulnerabilities'*.

The National Risk Assessment specifically highlights the following services to be at high risk of money laundering:

- Conveyancing
- Client account
- Trust and company formation

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.

We have produced a summary of the areas of the National Risk Assessment that are relevant to CLC Practices which you can find here.

Risk factors

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

Product/service

- Conveyancing

Conveyancing 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.

- 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.

- Trust and Company Service Providers (TCSPs)

Trusts or 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.

Client

Each client is different which will be reflected in their individual risk-profiles. 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)

The MLR 2017 extended the definition on PEPs to include PEPs from the UK. PEPs and their close families and associates must be identified and enhanced due diligence checks are required to mitigate the risks of corruption.

- 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.

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 can enable anonymity. 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

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.

Delivery channel

- Remote clients

Not seeing a client face-to-face 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.

- 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. 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 the reason for the payment before accepting funds.

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.

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 and knowledge of their services, clients and delivery channels.

We review practices' written risk assessments as part of our routine monitoring and inspections, or in response to specific information we receive.

You may find it helpful to have a look at the other AML resources the CLC offers.

Last reviewed: August 2018