Solicitors Regulation Authority

Guidance
Guidance
Proceeds of crime

Proceeds of crime

Updated 25 September 2023 (Date first published: 29 June 2023)

Status

This guidance is to help you understand your obligations and how to comply with them. We will have regard to it when exercising our regulatory functions.

This guidance uses 'must', 'should' and 'may' throughout - with the following meanings:

- **Must:** a requirement in legislation or a requirement of a regulation or other mandatory provision. You must comply unless there are specific exemptions or defences provided for in relevant legislation or regulations.
- **Should:** good practice for most situations. These may not be the only means of complying with the requirements and there may be situations where the suggested route is not the best option. If you do not follow the suggested route, you should be able to justify to us why your alternative approach is appropriate, either for your practice, or in the particular instance.
- **May:** an option for meeting your obligations or running your practice. Other options may be available and which option you choose is determined by the nature of the individual practice, client or matter. You may be required to justify to us why this was an appropriate option.

Who is this guidance for?

All SRA-regulated firms and those working within them, solicitors (including in-house solicitors), registered European lawyers and registered foreign lawyers.

It is important to note that:

- All firms have obligations under the Proceeds of Crime Act 2002 (PoCA), regardless of the services they provide, not just those within scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).
- PoCA imposes additional requirements on those in scope of the MLRs.

Purpose of this guidance

To help you understand how to prevent financial crime, help you understand the UK's proceeds of crime regime, and understand our expectations for how you comply with it.

Introduction

PoCA was introduced in the UK to help law enforcement agencies, such as the National Crime Agency, police services and HMRC, as well as other investigatory bodies tackle financial crime. It sets out:

- the proceeds of crime regime and the criminal offences of money laundering.
- obligations of reporting any suspected money laundering and terrorist financing activities.
- the concept of a nominated officer, also known as a money laundering reporting officer (MLRO).

While this guidance note deals with the PoCA regime, similar considerations also apply under the Terrorism Act 2000.

Does the Proceeds of Crime Act apply to me?

Yes. PoCA applies to everyone in the UK including all firms and individuals that we supervise. This is different to the MLRs, which applies to firms doing work in scope [https://www.sra.org.uk/solicitors/resources/money-laundering/guidance-support/scope-money-laundering-regulations/] of the regulations.

Proceeds of Crime Act 2002	MLR 2017
Applies to all firms	Applies only to firms offering services at a higher risk of being used to launder money
Applies automatically	Requires notification to the SRA before offering services in scope. Providing these services without proper approval is a breach

Sets out the underlying offences of money laundering and associated defences	Sets out regulatory requirements to prevent money laundering, including: risk assessment record keeping policies, controls and procedures internal controls.
Applies to: money real, personal, heritable or moveable property intangible or incorporeal property. Funds received in 'the ordinary conduct of litigation' are exempt from s.328	Generally only applies to clients' assets rather than payments for legal services
How firms comply with the act is up to them	Sets out a mandatory framework for compliance with certain minimum requirements for all firms in scope

Further guidance for those in scope of the MLRs can be found in the Legal Sector Affinity Group guidance [https://www.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf?version=496f8e] . This is referred to as being ‘in scope’ or ‘in the regulated sector’. If you are unsure whether you are in scope, we have published guidance [https://www.sra.org.uk/solicitors/resources/money-laundering/guidance-support/scope-money-laundering-regulations/] .

If your firm is out of scope, similar considerations may apply. For example, paragraph 8.1 of the Code of Conduct for individuals states that you must identify the clients for whom you act. To achieve this, you may consider adopting the requirements under the regulations for identification and verification of clients – and when deciding what approach to adopt should bear in mind factors such as:

- knowledge of the client
- the type of work involved
- whether instructions are taken from the client in person, online or via third parties
- the size and nature of the firm, its work and structure.

Similarly, paragraph 4.1 of the Code of Conduct for Firms states that you must only act for clients on instructions from the client, or from someone properly authorised to provide instructions on their behalf. This reflects regulation 28(10) of the MLRs, which sets out a requirement to identify and verify anyone representing a client, and to obtain the client's authority.

In general, though, a robust client identification process is one of the primary ways in which you can protect your firm from external threats such as impersonation and fraud. It is also the first line of defence against potential sanctions breaches, which can have very serious legal and regulatory consequences. We have produced specific guidance on complying with the sanctions regime [https://www.sra.org.uk/solicitors/guidance/financial-sanctions-regime/] which explores these issues further.

You should also consider the risk that individual clients and client matters may pose and may adopt more stringent checks accordingly. For example, if the client is established in a country subject to sanctions, this might include scrutiny of the source of any funds the client wishes to deposit in your client account, and open source checks in addition to identification.

The principal offences

The PoCA contains several offences related to proceeds of crime. The three principal offences are defined in sections 327, 328 and 329 of the act.

These offences do not need to involve money at all and can involve any proceeds of crime.

For example, under s.327, 'property' includes:

- money
- real, personal, heritable or moveable property
- intangible or incorporeal property. This could, for example, include intellectual property rights, cryptocurrency or non-fungible tokens.

1. Concealing etc (section 327)

A person commits an offence under section 327 PoCA if they:

- conceal criminal property
- disguise criminal property
- convert criminal property
- transfer criminal property
- remove criminal property from England and Wales or from Scotland or from Northern Ireland.

Property is deemed to be criminal if it was obtained through a criminal offence. 'Concealing' or 'disguising' criminal property includes concealing or disguising the nature of property, its source, location, disposition, movement or ownership or any rights.

A transfer of criminal property, for example, could include all of these things, as in this example below.

Illustrative example: sham litigation

Mr Jarndyce has embezzled £10m from his employer. He wants to make sure that the money is out of reach of law enforcement before this is discovered.

To do this he arranges for his accomplice, Mr Skimpole, to enter into sham litigation. Mr Skimpole approaches Mr Tulkinghorn, a solicitor, and instructs him that Mr Jarndyce owes him £10m and is refusing to pay. He produces fraudulent invoices as proof of this.

Mr Tulkinghorn writes to Mr Jarndyce, informing him that he is instructed by Mr Skimpole and that unless the matter is settled, will issue proceedings on his behalf.

Mr Jarndyce writes back, admitting that the money is owed, and offering to settle immediately. He requests the details of Mr Tulkinghorn's client account.

Mr Tulkinghorn provides client account details, and Mr Jarndyce pays the money in.

After deducting his fees, Mr Tulkinghorn pays the balance to Mr Skimpole – who has already asked for it to be paid to his USD account in an offshore tax haven. The receiving bank assumes it is legitimate money, as it is described as damages paid from a solicitor's client account.

The embezzled sum of £10m is therefore:

- **disguised** as payment of a legitimate debt

- **concealed** under a layer of legitimacy by the transfer in and out of a client account
- **transferred** from one party to another
- **converted** into another currency
- **removed** from the UK.

Mr Tulkinghorn should have:

- Been vigilant to suspicious activity, for example if the supposed debt was poorly evidenced, or when the matter settled unexpectedly quickly.
- Submitted a suspicious activity report as soon as suspicion arose (further details below on how to do this).
- Refused to transfer the funds overseas.

2. Arrangements (section 328 PoCA)

An offence is committed if a person enters into, or becomes concerned, in an arrangement they know or suspect facilitates (by whatever means) the:

- acquisition
- retention
- use or
- control of criminal property, by or on behalf of another.

'Arrangement' is not defined, and potentially involves a wide range of activity in money laundering offences. There are many ways legal professionals could be used in arrangements, such as:

- Sham litigation.
- Improper transfer or retention of funds, such as using client account as a banking facility.
- Improper transfer of restrained assets, such as sale of a property
- Sham arbitration, mediation or other firms of alternative dispute resolution.
- Use of client account or transfers of money to hide assets from creditors or the authorities.

3. Acquisition, use and possession (section 329 PoCA)

A person commits an offence under s.329 if they acquire, use, or have possession of criminal property. Firms do not need to do any more than hold the funds or assets they receive to commit this offence – it would be

enough that it passed through their custody or client account. Firms can help to prevent this by following our warning notice on using client account as a banking facility [https://www.sra.org.uk/solicitors/guidance/improper-client-account-banking-facility/] .

You may wish to make enquiries about the source of any funds your firm receives. By making reasonable enquiries, you can protect your firm against being used to hide the proceeds of crime.

Red flags

There are many warning signs that someone is trying to use your firm to obscure the origin of proceeds of crime. Some examples are given below:

- Unexplained secrecy from a client, and unwillingness to be open with their legal adviser.
- Vagueness about the source of any funds or how they were acquired.
- Litigation, arbitration or dispute resolution settling unexpectedly easily, particularly where large sums are at issue.
- Requests to pay funds, such as an award of damages, to third parties with no reason as to why the client could not make such a transfer themselves.
- Receiving instructions from unrelated third parties or intermediaries.
- Being asked to hold funds in escrow where there is no legitimate legal reason for this.
- Involvement with jurisdictions, or clients based in jurisdictions, which are known to be:
  - subject to international sanctions
  - tax havens
  - subject to corruption or political unrest
  - centres of the illegal drugs trade or terrorism.
- The firm being asked to work outside of its area of expertise or in an unfamiliar area of law without a reasonable explanation.

This is not an exhaustive list and firms must be aware that criminals are continually changing their approach to avoid detection.

Case study: R v Narinder Kaur, alias Nina Tiara

Ms Kaur was a serial fraudster, convicted at Gloucester Crown Court in March 2023. Among her various criminal activities she engaged in sham litigation on numerous occasions.

Ms Kaur would approach a firm of solicitors claiming that she wished to sue her brother for money owed to her. An accomplice posing as her brother would pay off the false debt using a fraudulently obtained credit card, paying the money into the firm's client account. The firm would then pay the money to Ms Kaur.

Sources

https://www.cps.gov.uk/west-midlands/news/serial-shoplifter-convicted-multiple-counts-fraud [https://www.cps.gov.uk/west-midlands/news/serial-shoplifter-convicted-multiple-counts-fraud]

https://www.bbc.co.uk/news/uk-england-gloucestershire-64965027 [https://www.bbc.co.uk/news/uk-england-gloucestershire-64965027]

Exemptions

The Court of Appeal case of *Bowman v Fels* ([2005] EWCA Civ 226 [https://www.bailii.org/ew/cases/EWCA/Civ/2005/226.html] established that s.328 (making arrangements) PoCA, is not intended to cover or affect the ordinary conduct of litigation by legal professionals. This protects actions taken by lawyers as part of legal proceedings enabling clients to take advice and pursue their rights in court and avoids creating an obligation to report matters that come to the attention of a lawyer during legal proceedings protected by legal professional privilege.

The judgment concluded that it was improbable that the UK legislator intended sections 327 to 329 to cover the ordinary conduct of legal proceedings or the ordinary giving of legal advice.

Handling assets in accordance with a judgment or alternative dispute resolution would not be a principal money laundering offence. For example, neither a victim who is receiving compensation and/or recovering their property following litigation, nor the lawyer facilitating this would be committing an offence under either s.327, 328 or 329 of the act. While the act of transferring the money is not illegal, the money itself would remain criminal property, meaning if it were to be used in a future transaction, for example buying a house, those acting in that transaction could be committing a POCA offence. If this situation arises, you should consider referring the client for specialist advice, as using the funds may commit an offence.

You should also note that that this exemption only applies to the **ordinary** conduct of litigation. Sham litigation, or a similar criminal enterprise, would not be covered by this as its intent is entirely criminal from the outset.

Suspicious activity reporting

The legal requirements in this area differ widely depending on whether the work is in scope of the MLRs. For in-scope work, please refer to the LSAG guidance [https://www.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf?version=496f8e] . For work out of scope of the MLR, please see below.

If you know or suspect that money laundering or terrorist financing has been, will be, or is in the process of being committed, you can help prevent crime and protect yourself against prosecution under PoCA by making a suspicious activity report (SAR) to the National Crime Agency (NCA) through an online portal. [https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports] This remains subject to legal professional privilege (LPP), which is explored in more detail below.

SARs play a crucial role in helping law enforcement identify criminals, locate illicit funds or assets, and understand the methods being used by money launderers and other criminals. They can also stop crimes in action and help protect vulnerable persons from being exploited, therefore information you provide in your SARs may prove to be invaluable in investigations.

The threshold for suspicion is low and involves: 'a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds'.' (*R v Da Silva* [2006] EWCA Crim 1654 [https://www.bailii.org/ew/cases/EWCA/Crim/2006/1654.html]).

Firms which do not carry out work in scope of the MLRs do not have to appoint a MLRO, though we strongly recommend that they do. The advantage of doing so is to concentrate responsibility in one place and provide clarity for members of staff on who to go to if they have any suspicions. The MLRO can advise and assist members of staff with submitting a SAR, minimising the number of unnecessary reports. We would expect an out-of-scope firm which decides not to appoint an MLRO to have suitably robust systems and controls in place to detect and prevent money laundering, similar to those set out in the money laundering regulations.

The role of the MLRO holds considerable responsibility immediately upon appointment. Under s.332 PoCA [https://www.legislation.gov.uk/ukpga/2002/29/section/332] , an MLRO commits an offence of failure to disclose:

- If they know or suspect that another party is engaged in money laundering.

- If the information came to the MLRO as an authorised or protected disclosure under ss.337 and/or 338.
- If the MLRO identifies a person or assets involved in money laundering, or could help to identify them.

How to submit a SAR

SARs should be clear, as detailed as possible, and set out why you are suspicious. You should assume you are writing for a non-lawyer reader and explain any legal terms or concepts. It is also important to include contact details such as email addresses, telephone numbers and bank account details.

There are two types of SAR which can be submitted to the National Crime Agency (NCA):

An information-only SAR.

This could include:

- Suspicion or knowledge about a prospective client who did not instruct the firm.
- New information has come to light since an event or transaction has already happened which has led to forming a suspicion.
- The suspicion concerns a third party such as the client of another firm or a non-client involved in a matter.

This kind of SAR is generally appropriate where a transaction or event has already occurred, but the circumstances made you suspicious and this is therefore reported to the NCA to help them build an intelligence picture. It may also be appropriate where you become aware of suspicious activity on the part of a third party to a matter, for example the counterparty.

If you are in the process of acting for a client, however, you will need to cease acting or submit a defence against money laundering.

A defence against money laundering (DAML) SAR:

This is where you are seeking consent to continue with a transaction that may involve the proceeds of crime. For example:

- a client cancels their instructions and requests a repayment after depositing a large sum of money with the firm
- a client insisting that sums due to them are instead paid to a third party
- the payment of damages in a case which has settled suspiciously easily.

If granted, the DAML means that the NCA gives consent for the proposed potentially criminal act to take place. They provide a defence against committing money laundering offences ss.327-329 of PoCA. They do not:

- oblige the reporter to carry out the prohibited act and you may choose not to proceed
- legitimise the funds
- override private rights of an individual
- override or replace regulatory requirements
- prevent law enforcement investigating the subject.

The permission granted by a DAML is limited to the proposed transaction or course of action set out in the SAR – for example, having consent granted in one instance does not cover any future instances, even if the circumstances appear exactly the same. There is also no guarantee that a subsequent DAML would be granted.

Once you submit a DAML, the NCA has seven working days to assess the SAR and ask for more information if necessary. This is known as the 'notice period' and starts the day **after** submission.

There are four possible outcomes from submitting a DAML. The NCA can:

1. grant consent, and you may carry out the proposed course of action
2. refuse consent and you will enter a moratorium period of a further 31 calendar days
3. request further information
4. not respond in the seven-day period. If this happens, you may consider that you have deemed consent under s.335(2) PoCA.

If you need consent sooner, you should clearly state the reasons for the urgency in your SAR. Within the notice and moratorium period you must not undertake a prohibited act. However, this does not prevent you taking other actions on the file, such as writing letters, conducting searches etc.

Finally, please also note that submission of either type of SAR does not absolve you from any other reporting requirements, including:

- reports to the SRA of another solicitor's misconduct
- reports to the Office of Financial Sanctions Implementation of sanctions breaches.

What if my firm does not have a nominated officer/MLRO?

Only MLROs are required to make disclosures if they know or suspect that money laundering or terrorist financing has occurred.

Any person, however, can make a SAR under ss.337 and 338 PoCA which will protect you using the NCA's online SAR reporting system [https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports] . If you do this, however, you will have to keep your own records and ensure that they remain confidential to those who need to know.

As mentioned above, we recommend that all firms appoint an MLRO. Aside from making disclosures, an MLRO can oversee the firm's compliance and make sure that it does not commit any PoCA offences.

Tipping off and prejudicing an investigation

Under s.333A, it is an offence to inform the subject of a SAR that a report has been made, but only if the conduct reported is within the AML regulated sector as set out in regulations 11 and 12. For more information, see our guidance [https://www.sra.org.uk/solicitors/resources/money-laundering/guidance-support/scope-money-laundering-regulations/] .

If your firm does not work in the regulated sector, however, you should still think carefully before informing the subject of a SAR that one has been made. To do so could be a breach of the law and your professional obligations. Disclosing that a SAR has been submitted could also ultimately place you and those in your firm in danger of harm.

Prejudicing an investigation is also an offence under s.342 PoCA, and a person commits an offence if they make a disclosure that is likely to prejudice an investigation or tampers with (or permits others to tamper with) documents that are relevant to an investigation.

SARs are documents of the utmost confidentiality, and the system will only work if this is maintained.

Legal professional privilege (LPP) and litigation privilege (LP)

The question of when LPP and LP arise in relation to PoCA is extremely complex, and what follows is a summary of the key points involved. A full explanation can be found in more detail in the LSAG guidance [https://www.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-guidance.pdf?version=496f8e] . The same overarching principles apply to work that is both in and out of scope of the MLRs. Note that the guidance on

'privileged circumstances under s.330 PoCA' does not apply to activity that is out of scope of the MLRs.

The application of legal professional privilege is often complex and fact sensitive. You should also bear the following points in mind:

- If you are in any doubt as to whether LPP applies in the context of the case in which you act, you should seek independent legal advice as part of your decision-making process.
- Seeking legal assistance in this manner, or assistance from your MLRO, does not constitute a breach of your retainer with the client, the rules of professional conduct or the provisions of PoCA or the MLRs.
- Sections 327(2)(b), 328(2)(b) and 329(2)(b) all provide a defence of having a reasonable excuse for not making a disclosure. It is therefore good practice to record the rationale for any decision. This will provide evidence of the decision-making process and may, in addition, assist in any consideration of a defence in the future, meaning you would be well placed to defend your firm's conduct to law enforcement or in the event of a regulatory investigation.
- LPP is negated by an attempt to use it to further a criminal offence.

What does a good proceeds of crime regime look like?

A realistic view of risk

One of the major failings we see in law firms is complacency, where firms assume that the risk of becoming involved in the proceeds of crime is automatically low.

- **All firms are at risk.** Criminals can target any firm irrespective of its profile, its history, its reputation or its location.
- **Firms who do not hold client money are also at risk.** A firm's office account can also be used to launder money as well as a client account.
- **Criminals come in many guises.** They may be long-standing clients, or indeed friends, where trust has led a firm to be lax in its procedures. They may be new clients, with an unknown background. They may present as wealthy, or in straitened circumstances. They may be a foreign oligarch or a small-time local drug dealer. They may hide behind intermediaries or nominees. A stereotyped view of criminals can lead to red flags being missed, but applying the same rigorous identification measures to all clients will help to mitigate this risk.

Appoint a money laundering reporting officer

PoCA provides a defence under ss.337 and 338 if a report has been made to a nominated officer – more commonly known as the MLRO.

The MLRs requires all firms in scope to appoint an MLRO – it remains optional for firms out of scope. We recommend, though, that all firms consider doing this so that they can take advantage of the protection afforded by PoCA, streamline their reporting, and help manage threats to the firm.

Once a report has been made to an MLRO, it is the MLRO's responsibility to decide whether a SAR needs to be made. An MLRO will therefore need:

- a thorough understanding of the firm and its work
- a good working knowledge of legal professional privilege and when it applies
- authority and the ability to make independent, accountable and possibly unpopular decisions
- unrestricted access to the firm's information systems.

Our thematic review, *Money Laundering Governance: Three Pillars of Success* [https://www.sra.org.uk/sra/research-publications/money-laundering-governance-three-pillars-of-success/] , gives further information on the appointment and role of MLROs in the regulated sector. The principles of this guidance also apply outside the regulated sector. We also strongly recommend that all firms appoint a deputy MLRO, for both holiday cover and succession planning.

A policy on reporting

All firms should have a policy on reporting suspicious activity, whether they are in scope or not. This should include:

- a definition of knowledge and suspicion
- the consequences of failure to report
- the identities of the MLRO and Deputy MLRO, and how to contact them
- what should happen once a report has been made.

Good record-keeping

The MLRO should keep a record of all internal reports made to them, as well as any SARs submitted.

This will allow the MLRO to evidence any decisions if they are called into question, as well as to keep track of any trends. Any documents relating to SARs should be kept separately to the client file. This reduces the risk of SARs being mistakenly disclosed to the client.

We have encountered several different ways of making internal reports, all with their own pros and cons. These include the use of standardised forms, reports through managers, and direct conversations.

We suggest a hybrid approach is likely to be most effective, such as an initial verbal report to the MLRO who will then decide if a report to the NCA is:

- not needed, in which case the conversation is summarised in email, recorded and archived by the MLRO
- needed, and the reporter is asked to fill out a standard form for submission to the MLRO.

This makes sure that fee-earner's time is only spent when needed and that the MLRO has all of the information they need to take the matter forward. We strongly recommend that reports be made directly to the MLRO without any intervening layers of management.

Well-trained staff

All staff, not just fee-earners, should have an understanding of:

- the relevant parts of PoCA and the obligations it places on firms and individuals
- the warning signs they should look out for when dealing with clients and client matters
- how they can report suspicious activity within the firm.

This last point is crucial - every firm will differ on how they wish staff to make reports, and all staff members should know how to do this at short notice if required.

For further information about the impact of submitting a SAR on confidentiality where your firm is outside of the regulated sector and does not have an MLRO, you may also wish to consult our guidance [https://www.sra.org.uk/solicitors/guidance/confidentiality-client-information/] . This sets out our stance where a disclosure has been made to prevent commission of a crime, or where there are safeguarding concerns including modern slavery.

Other resources

- Our warning notice on suspicious activity reports [https://www.sra.org.uk/solicitors/guidance/money-laundering-terrorist-financing-suspicious-activity-reports/]
- Legal Sector Affinity Group guidance [https://www.sra.org.uk/globalassets/documents/solicitors/firm-based-authorisation/lsag-aml-

guidance.pdf?version=496f8e]

- NCA: Submitting better quality SARs [https://www.nationalcrimeagency.gov.uk/who-we-are/publications/650-guidance-on-submitting-better-quality-suspicious-activity-reports-sars-v9-0/file]
- Money Laundering Governance: Three Pillars of Success [https://www.sra.org.uk/sra/research-publications/money-laundering-governance-three-pillars-of-success/]
- Use of client account as a banking facility: case studies [https://www.sra.org.uk/solicitors/guidance/improper-use-client-account-banking-facility/]