MONEY LAUNDERING POLICY

Glossary

AML	anti-money laundering
CDD	client due diligence
CTF	counter-terrorist financing
MLCO	money laundering compliance officer
MLR 2017	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by the Money Laundering & Terrorist Financing (Amendment) Regulations 2019
MLRO	money laundering reporting officer (also known as a nominated officer)
NCA	National Crime Agency
ongoing monitoring	review of retainers, including the source of funds, to ensure that they are consistent with our knowledge of the client, their business and risk profile
POCA 2002	Proceeds of Crime Act 2002
SAR	suspicious activity report (also known as a disclosure)
warning signs	features of retainers which may suggest that money laundering or terrorist financing is taking place
DAML	defence against money laundering (also known as consent)
EUFS	European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017
CFA	Criminal Finances Act 2017
OFSI	Office of Financial Sanctions Implementation

Money Laundering and Financial Regulations

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended), which implement the EU Fifth Anti-Money Laundering Directive and the new CDD requirements.

- Amendments to the Proceeds of Crime Act 2002 brought in by the Criminal Finances Act 2017 relating to Further Information Orders and changes to the moratorium period for Suspicious Activity Reports.

- European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017.

Purpose

This policy and the related procedures set out how KPM will achieve compliance with its legal and regulatory obligations under the AML/CTF and Sanctions regimes.

All employees and partners must familiarise themselves and comply with this policy and related procedures. Failure to do so may result in disciplinary action because of the risks associated with non-compliance, and may also result in criminal sanctions for the employees, managers and partners involved.

Solicitors are key professionals in the business and financial world, facilitating vital transactions that underpin the UK economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose.

KPM must safeguard against becoming involved in the processing of illegal or improper gains for clients.

As a professional practice KPM is particularly attractive to criminals wishing to convert gains to a respectable status. It is the policy of KPM not to assist them to do so. To do so could in any event be an unlawful act on the part of anyone concerned and could place KPM and its representatives at risk of criminal and civil proceedings.

Application

This policy applies to all partners and employees of KPM including those undertaking work through a consultancy arrangement, in a volunteer capacity, on a temporary basis, or through an agency.

All areas of practice must comply with the procedures designed to avoid the commission of any money laundering or terrorist financing offences.

Definition of Money Laundering

Money laundering is generally defined as the process by which proceeds of crime and the true ownership of those proceeds are changed so that the proceeds appear to come from a legitimate source.

The signs to watch for:

- **Unusual settlement requests:** Settlement by cash (or attempts to do so) of any large transaction involving the purchase of property or other investment should give rise to caution. Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and a prospective investor should give rise to additional enquiries.

- **Unusual instructions:** Care should always be taken when dealing with a client who has no discernible reason for using KPM's services, e.g. clients with distant addresses who could find the same service nearer their home base, or clients whose requirements do not fit into the normal pattern of KPM's business and could be more easily serviced elsewhere.

- **Unexpected and confusing changes to instructions:** Particular care is needed in relation to abortive transactions, surprisingly generous payments being made to supposed opponents or instructions that change for no obvious reason.

- **Large sums of client money:** Always be cautious when requested to hold large sums of money in client account, either pending further instructions from the client or for no other purpose than for onward transmission to a third party.

- **The secretive client:** A personal client who is reluctant to provide details of his or her identity. Be particularly cautious about the client you do not meet in person in which case 'enhanced customer due diligence' is required.

- **Suspect territory:** Caution should be exercised whenever a client is introduced by an overseas bank, other investor or third party based in countries where production of drugs or drug trafficking may be prevalent.

Money Laundering Compliance Officer

Matthew Stubbs has been appointed Money Laundering Reporting Officer (MLRO) and additionally as Money Laundering Compliance Officer (MLCO). His duties in this regard are to:

- Ensure that satisfactory internal procedures are maintained.
- Arrange for periodic training for all relevant personnel within KPM.
- Provide advice when consulted on possible reports and receive reports of suspicious circumstances.
- Report such circumstances, if appropriate, to NCA on behalf of KPM.
- Direct colleagues as to what action to take and not take when suspicion arises and a disclosure is made.
- Report annually to the Partners on the operation of the anti-money laundering policy and procedures.

The MLRO is responsible to the Partners for oversight and implementation of this policy and the relevant procedures and for providing guidance and assistance to KPM.

The MLRO is solely responsible for the decision to make SARs to the NCA and is the only person authorised by KPM Solicitors LLP to make SARs to the NCA.

The MLCO is the officer responsible for the practice's compliance with the current Money Laundering Regulations.

Principles

All employees and partners must:

- conduct CDD as required by law and set out in the relevant procedures;
- monitor all retainers on an ongoing basis for warning signs of money laundering or terrorist financing;
- seek guidance from the MLRO/MLCO on CDD issues;
- see guidance from the MLRO/MLCO if they have concerns about a client or retainer;
- report any warning signs regarding clients or specific retainers in accordance with the procedure for making SARs;
- refer any queries or requests for information from law enforcement to the MLRO in accordance with the procedure for responding to law enforcement requests;
- follow directions received by the MLRO;
- maintain confidentiality;
- avoid discussing any potential or actual reports with clients or third parties unless authorised to do so by the MLRO;
- ensure they do not engage in money laundering or facilitate terrorist financing.

Responsibilities

It is the duty of all personnel within the practice to:

- Be aware of their AML/CTF/Sanctions obligations.
- Comply with this policy and related procedures.
- Attend training arranged within KPM if required to do so.
- Conduct identity checks and other due diligence enquiries (CDD) on a timely basis unless the MLRO signifies that this is not necessary in the particular case in hand.
- Report without delay all circumstances which could give rise to suspicion that KPM is being involved in some element of the money laundering process for a client.
- Be wary of payment arrangements different from those anticipated or deposits of cash into client account.
- Follow the directions of the MLRO when a disclosure has been made, bearing in mind the personal risk to the adviser of 'tipping-off' the client in question either expressly or by implication.
- Maintain the utmost caution in maintaining confidentiality for the client and KPM when suspicious circumstances arise.

The Money Laundering Reporting Officer and disclosures

A disclosure could be necessary for one of three reasons:

- First, the Proceeds of Crime Act 2002 (POCA 2002), s.330 (as amended by CFA 2017), imposes a duty to make a disclosure if, in the course of practice, a person forms a suspicion (or should reasonably have done so) that money laundering is or could be occurring. The position is complicated by the fact that this is stated to be limited to the 'regulated sector' and is subject to the defence of legal professional privilege. The defence of privilege will mean that in most circumstances there is no need for the practice to make a report to the National Crime Agency (NCA) on the basis of instructions received. This is not always the case, however, and the Partners therefore take the view that any knowledge or suspicion that is formed of money laundering in relation to any activities within KPM must be reported under KPM's internal reporting procedure.

- Secondly, it should be noted that a disclosure might also be necessary to gain a defence to a charge under the principal offences under POCA 2002, ss.327–329, (as amended by CFA 2017), most probably that of entering into an arrangement whereby money laundering is facilitated under s.328. There are similar offences in Terrorism Act 2000, ss.15–18. Where a suspicion arises KPM may, subject to the complex provisions relating to legal professional privilege, need to make a disclosure and gain permission to continue to act. Since the rules on the need to make a disclosure are complex and, following the leading case of *Bowman* v. *Fels* [2005] EWCA Civ 226, are different as between contentious and non-contentious work, it is the policy of KPM that all concerns and suspicions must be discussed with and then possibly reported to the MLRO.

- Thirdly, a terrorist financing offence (sections 15-18 of the Terrorism Act 2000 (TACT) (as amended by MLR 2017) under section 21za of TACT) (as amended by MLR 2017 and subject to EUFS 2017).

Please also note that:

- The duty to disclose extends to all 'criminal conduct' that results in 'criminal property' (for the statutory definition of these terms and others used for liability see POCA 2002, s.340).

- In general there are no de minimis provisions: any criminal activity, however menial the gain, must be reported for a person to be sure that (s)he has discharged their responsibility.

- **The law makes no distinction between fee earners, administrators and secretaries.**

- This duty is not confined to disclosure in respect of clients – POCA 2002, s.330 sets out a duty to make a disclosure where a person has a knowledge or suspicion of money laundering, or should reasonably have done so, in respect of 'another person'. In practice this will often be the opponent.

- There is no positive duty under POCA 2002, s.330 for anyone to report suspicions that arise in their personal life – merely their professional activities – but the principal offences in POCA 2002, ss.327–329 apply generally and not just to those who work in the regulated sector.

- Part 1 of the Serious Crime Act 2015 came into force on 1 June 2015 to strengthen POCA in relation to third party interests and to strengthen POCA asset recovery – since then the MLR 2017, EUFS 2017 and CFA 2017 have also been brought into force.

The Partners have determined that **all work conducted by KPM should be regarded as being covered by the Money Laundering Regulations with the consequential need to conduct identity and address checks**.

A report of suspicious circumstances must be made to Matthew Stubbs on Internal Report Form (found at Annex 1E), who will:

- Consider the information and make such further enquiries as are necessary to form a view on whether a report to the authorities is needed.
- Ensure that nothing done by KPM could alert the client in question that a report and an investigation could ensue.
- Make a disclosure, if appropriate, making full notes of the reasons for doing so and in accordance with the NCA online reporting process. The link to that website is as follows:
  http://www.nationalcrimeagency.gov.uk/publications/713-requesting-a-defence-under-poca-tact/file
- Make diary notes in KPM's key dates system of when KPM may continue to act (see the provisions on deemed consent to continue after seven working days at POCA 2002, ss.335–336) and direct the adviser further as appropriate.
- Consider whether the intended subject of a disclosure, if a client, needs to be consulted about the planned disclosure for permission to use the privileged information that forms the knowledge or suspicion leading to the need for a disclosure.
- Co-operate with any production orders made by the proper authorities.
- Maintain all records of disclosures and reports for at least five years.

In certain circumstances advisers may or must report to the client that a disclosure will be made.

They might also sometimes have the option of informing a client that a disclosure has been made concerning them, notwithstanding the offences of 'tipping-off' (POCA 2002, s.333) and 'prejudicing an investigation' (POCA 2002, s.342) under the defence of legal professional privilege.

Generally, informing the subject about a disclosure would amount to the crime of 'tipping-off' under s.333 where a disclosure has already been made (there is a similar offence in s.342 of informing the person before a disclosure is made where an investigation is pending).

However, these offences provide for the defence of legal professional privilege. After some dispute the courts have ruled, in effect, that privilege will be valid and excuse a disclosure to the client as long as the adviser is acting in good faith and there is no criminal purpose on their part. The actual position is very much more complex than this and KPM has determined that the **consent of the MLRO is needed if any member of staff intimates to any person in any way that a disclosure to the authorities has been or will be made**.

Clearly, a person who does not disclose when they should do is at risk of prosecution, but a person who discloses when they should not do so could be in breach of their normal professional duties to the client.

KPM have subscribed to e-alerts to any changes to the Financial Sanctions Targets List of all asset freeze targets. Karen South, Matthew Stubbs and Louise Axon all receive e-alerts of any changes.

By subscribing to the Sanctions Targets List, KPM are provided with information to help us decide whether or not we are dealing with someone who is subject to sanctions. It lists:

- Full name;
- Any known aliases, honorary, professional or religious titles;
- Date of birth;
- Place of birth;
- Nationality;
- Passport details
- National identification numbers, e.g. ID cards, social security numbers;
- Address;
- Any additional information that may be useful, e.g. nicknames, details of family;
- Title of the financial sanctions regime under which the designated person is listed;
- The date when the designated person was added to the list by HM Treasury;
- When the information regarding the designated person/entity was last updated by HM Treasury;
- A unique ID reference number relating to the designated person identity.

You will find the Financial Sanctions Guidance March 2018 at: P:LEXCEL:Anti-Money Laundering: Financial Sanctions Guidance. Chapter 5 refers to your reporting obligations.

In accordance with the Guidance, legal professionals **MUST** report to the OFSI (as soon as practicable) if we know or have reasonable cause to suspect that:

- A person is a designated person.
- Has committed an offence under the Regulations.

We are required to report this information or other matter on which our knowledge or suspicion is based if it came to us in the course of carrying on our business.

When reporting to the OFSI we must include;

- The information or other matter on which the knowledge or suspicion is based.
- Any information we hold about the person or designated person by which they can be identified.

If we know or have reasonable cause to suspect that a person is a designated person and that person is a client of KPM, we must also state the nature and amount or quantity of any funds or economic resources held by us for that client.

Reporting Procedure Table

Reporting Area	**Example**
Person is a designated person	A customer or client of yours is a designated person. You must provide OFSI with any information you hold about the designated person by which they can be identified.
Offences	Exact offences will depend on the particular legislation, but can include: • making funds or economic resources available to a designated person (except where an exemption applies or under licence) • dealing with funds or economic resources that must be frozen (except where an exemption applies or under licence) • activities that circumvent an asset freeze • breaches of licensing conditions
Funds and economic resources	You must include details of any funds and economic resources that you have frozen.
Credits to frozen account	A relevant institution must inform OFSI without delay whenever it credits a frozen account with: • payments due under prior contracts • payments made under judicial decisions rendered in an EU member state • funds transferred to an account by a third party

UK Financial Sanctions Regimes

The UK's domestic regimes carry similar reporting obligations for KPM as mirrored by the EU Regulations above. There is no general obligation to report under the UK domestic regimes but in spite of this, the obligations to comply with Financial Sanctions still applies.

How to Report

Reports of frozen funds and economic resources, information regarding a designated person, notification of credits to frozen accounts should be emailed to: ofsi@hmtreasury.gsi.gov.uk.

Reports regarding suspected breaches should be submitted to OFSI using the form at: www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do.

OFSI will handle all information it receives in accordance with the relevant sanctions legislation and the Data Protection Act 1998.

Legal Professional Privilege

Both the EU Regulations and the UK domestic regimes make clear that the reporting requirements do not apply to information to which legal professional privilege is attached. However, OFSI expects KPM to carefully ascertain whether or not legal privilege applies and which information it applies to.

OFSI may challenge a blanket assertion of the legal professional privilege – where it is not satisfied that such careful consideration has been made.

All such matters must be referred to the MLRO who will then take a decision as to obtaining advice as to the position of legal professional privilege as regards KPM and its business relationship and client relationship.

Please note that:

- There are two forms of privilege – advice and litigation.
- The Law Society advice also distinguishes common law privilege from the statutory format of privilege referred to in POCA 2002.
- The Internal Report Form invites you to comment whether you think a disclosure should be made – only complete this part of the form if you feel competent to comment.

You must not intimate to the client in any way that a disclosure will be made or has been made to the MLRO or to NCA unless and until you receive instructions to do so.

Do not store a completed Internal Report Form on the matter file to which it relates. This would create a risk that the client might see the disclosure report. To alert all personnel to the fact that a disclosure has been made, however, and that KPM may do no more for the client until it has permission to proceed, you must:

- Place the file in the hands of the MLRO when you have made a report (who will maintain control of the file).
- Retrieve the file from the MLRO says that you may continue to act.

If in doubt or requiring further clarification, speak with the MLRO and/or review the following link to the NCA website:

http://www.nationalcrimeagency.gov.uk/publications/713-requesting-a-defence-under-poca-tact/file

Evidence of identity

Advisers must obtain evidence of identity for all clients as soon as possible after contact is first established between KPM and the potential client.

- The Law Society guidelines make the distinction between ‘identification’ (being told or coming to know a client’s identifying details) and ‘verification’ (obtaining some evidence which supports this claim of identity).
- In general ‘customer due diligence’ requires both elements to be addressed. Exceptions to these requirements can only be sanctioned by the MLRO.
- Fee earners must note that they should not take a colour copy of a passport because this in breach of Section 163 of the Copyright Designs and Patents Act 1988
- The evidence of identity check must be placed on the client file at the time of each matter opening of the client in question, unless excepted by MLRO.
- There are also obligations to check for beneficial ownership and to investigate the control and management arrangements in certain cases.
- It would be prudent at this point to obtain a copy bank statement from a client to add to the verification process in relation to money transferring out of KPM to the client.

The bank statement will contain the sort code and account number by way of confirmation.

Please note that:

- Every attempt should be made to meet the client in person to verify the evidence provided;
- Where this is not possible the client **should not** be asked to send their passport or driving licence through the post. In these circumstances the adviser should query why a client is unwilling to meet him/her. If there is a valid reason (usually geographical) it is better to obtain certification through local solicitors or other professionals: in these circumstances the adviser must make a check of the validity of the referring firm or organisation in a current directory and note the identification on file.

In the case of commercial clients (i.e. non-human clients Company entities):

- A copy of the certificate of incorporation must be obtained at the outset of the first matter for that client.
- Along with a companies search or evidence of the identity of two directors or officers, if possible, unless the representatives are known to KPM and have had personal ID checks already.
- Further checks may be needed in the case of non-domiciled companies. It is, in any case, important to check that those who purport to represent an organisation are actually entitled to do so.
- Beneficial ownership checks – you must establish the veracity of the information given in respect of a company and details of the steps you need to take are cross-referenced in the following checklists:
  Annex 8A2 Private Client Verification Checklist
  Annex 8A4 Entity or Legal Arrangement Client Verification Checklist
- Annex 8A1 Private Client Inception Form also seeks further information as to the beneficial ownership.
- On every matter where a limited company is the client, then Companies House should be accessed to check the situation with regards to the registered Directors and any other matters of concern.
- PSC Register.
- Cross-reference your obligations under Financial Sanctions and in particular, refer to Chapter 4 of the Financial Sanctions Guidance March 2018.

The Partners recognise that many clients may resist the request for evidence of identity, but clients should be reassured that this is now standard practice for any financial or professional concern and that there is no choice over it, unless the adviser wishes to risk prosecution for non-compliance with the MLR.

KPM's client care letter now reflects the need for identity to be checked and this wording may also assist to reassure clients that our actions are not taken because we mistrust them.

In relation to established clients, the **current address** should always be checked in relation to any new instructions.

If your client has moved address, then the original CDD may not be valid and the whole process must be undertaken if there is a change in that original CDD compliance.

KPM have subscribed to a service known as Experian Prove ID which allows KPM to verify the identity of individuals in real time providing a fast and secure environment for KPM and their clients.

KPM will also seek to verify bank account details given by a client where there is to be a transfer of money out of KPM to the respective client. The detail of this policy is contained in financial management under 3.10.2.

KPM also carries out screening of its employees as regards identity verification – both photographic and residence together with qualifications and suitability for the role within KPM.

KPM also take up references and make relevant enquiries with the applicant's professional bodies including the Law Society, the SRA, ILEX, CLC and the Faculty Office.

KPM will also use Experian ID to identify their employees and will take DBS searches when and if appropriate (once the relevant consent has been obtained).

Records

KPM is obliged to maintain records for at least five years of:

- What has been done for the client.
- Any disclosures made (completed Internal Report Form).

Please bear this in mind when deciding a destroy date when archiving files.

In addition KPM must maintain ID evidence for at least five years from the end of the 'business relationship' or the close of the 'occasional transaction'. On file closure, the certified copies of ID documentation are saved onto KPM's case management system before the hard copies are shredded. The ID is then kept on the case management system for a period of 10 years before it is removed and destroyed.

The Osprey case management system now has a provision for the fee earner to insert a data retention period and periodically a report will be run to ascertain what data can be eradicated and removed.

Audit of AML Policies, Controls and Procedures

The KPM Controls and Procedures are monitored and evaluated by our Auditors on an annual basis. The Auditors have a separate function of reviewing our controls and procedures as part of the audit process.

Related policies and procedures

The following policies and procedures must be considered when complying with this policy:

- file opening;
- disciplinary procedure policy;
- annual appraisal policy;
- appointment and role of the MLCO;
- appointment and role of the MLRO;
- AML/CTF risk assessment;
- client identification and verification;
- ongoing monitoring;
- making SARs;
- responding to requests for information from law enforcement;
- exiting client relationships – AML/CTF considerations;
- accepting cash and monitoring accounts – AML/CTF considerations;
- record-keeping;
- AML/CTF training;
- monitoring AML/CTF compliance.

Date of effect/date of review

This policy came into effect on 1 May 2018. This policy shall be reviewed annually.