Anti-Money Laundering and Counter-Terrorist Financing Policy

1st February 2012
1st Review 8th June 2012
2nd Review Date 16th May 2013
3rd Review Date 3rd June 2014
4th Review Date 19th May 2015
5th Review Date 20th May 2016
6th Review/ Revision 27th July 2016
7th Review/Revision 30th August 2017
8th Review/Revision 28th March 2018
9th Review/Revision 20th February 2019
10th Review/Revision 17th April 2019
11th Review/Replaced 3rd December 2019
12th Review/Revision 22nd January 2020
13th Review/Revision 18th June 2020
14th Review/Revision 5th November 2020
15th Review/Revision 4th March 2021
16th Review/Revision 21st April 2021

Contents

1 Introduction to the policy 1

2 Scope and application 1

3 Responsibility for anti-money laundering and counter-terrorist financing compliance 1

4 Failure to comply with this policy 2

5 Accounts procedures 2

6 What are money laundering and terrorist financing? 2

7 Money laundering/terrorist financing warning signs 3

8 Money laundering offences 6

9 Terrorist financing offences 10

10 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, (MLR 2017), as amended 11

11 Reporting suspicions 11

12 CDD–what is client due diligence? 14

13 CDD—who is the client? 14

14 CDD—in which situations is CDD required? 15

15 CDD—in what time frame must CDD be completed? 16

16 CDD process 16

17 CDD records 21
18 CDD—different levels of CDD 21
19 Enhanced due diligence 22
20 CDD—high-risk third countries 23
21 CDD—politically exposed persons (PEPs) 24
22 EDD—complex or unusual instructions 26
23 EDD measures for other high-risk clients 26
24 Senior management approval 27
25 Regular due diligence (RDD) 27
26 CDD—beneficial owners 27
27 CDD—source of funds 29
28 CDD—purpose and intended nature of the business relationship 30
29 What happens if I cannot conclude the CDD exercise? 30
30 CDD—relying on a third party to conduct CDD 31
31 CDD—reliance on our CDD by another firm 31
32 Reporting discrepancies in CDD information 31
33 CDD—ongoing monitoring 32
34 Receiving funds from the client or a third party 34
35 Responding to investigations 35
36 Screening relevant employees 35
37 Training and awareness 35
38 Monitoring and reviewing this policy 36
39 Further information 36
Appendix 1 Internal suspicious activity report form 37
Appendix 2 Client due diligence matrix 41
Appendix 3 Source of funds statement 74

1 Introduction to the policy

1.1 Stephen Rimmer LLP is required to put in place appropriate systems and controls to combat money laundering and terrorist financing under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (MLR 2017), as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/1511, and from 6 October 2020, the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020, SI 2020/911.

1.2 For more details on the MLR 2017, see section 10.

2 Scope and application

2.1 This policy contains the procedures we have developed to comply with the MLR 2017, as amended.

2.2 This policy applies to all our offices, employees, officers, consultants, contractors and to other workers including agency workers, interns and home workers.

2.3 All staff must be familiar with this policy and comply with its terms.

2.4 This policy does not form part of any contract of employment and we may amend it at any time.

3 Responsibility for anti-money laundering and counter-terrorist financing compliance

3.1 The firm itself is primarily responsible for compliance with the MLR 2017, including all systems and control requirements.

3.2 We have appointed a board-level officer as the officer responsible for compliance with the MLR 2017— Andrew Flagg

3.3 Our nominated officer Andrew Flagg has a separate responsibility to:

3.3.1 receive and assess suspicious activity reports (SARs)—see section 11; and

3.3.2 determine whether the SAR gives rise to knowledge or suspicion (or reasonable grounds for knowledge or suspicion) that a person is engaged in money laundering or terrorist financing.

3.4 For practical expediency, our nominated officer also has responsibility for wider compliance with AML and counter-terrorist financing compliance and other areas of crime prevention, including in relation to:

3.4.1 risk assessment;

3.4.2 client due diligence;

3.4.3 systems and controls;

3.4.4 staff training and awareness;

3.4.5 monitoring and review;

3.4.6 reporting CDD discrepancies;

3.4.7 anti-bribery and corruption—see our separate Anti-bribery and corruption policy;

3.4.8 fraud prevention;

3.4.9 financial sanctions;

3.4.10 tax evasion; and

3.4.11 organised crime.

4 Failure to comply with this policy

4.1 Failure to comply puts both you and the firm at risk.

4.2 You may commit a criminal offence if you fail to comply with this policy. The AML and CTF regimes carry heavy criminal penalties ranging from two years' imprisonment for failing to apply appropriate CDD measures to 14 years' imprisonment for committing a principal money laundering or terrorist financing offence.

4.3 We take compliance with this policy very seriously. Because of the importance of this policy, failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

5 Accounts procedures

5.1 We have robust systems to ensure that the firm's office and client bank account details are only disclosed to clients and third parties where necessary.

5.2 All managers and staff must understand that:

5.2.1 members of the Finance department must not be pressurised into actions or omissions that place the firm at risk of involvement in financial crime;

5.2.2 where a member of the Finance team has concerns about a matter or transaction, they are expected to consult their manager, the COFA or nominated officer;

5.2.3 the Finance team will always consult the nominated officer before taking steps to return any unidentified funds to the originator; and

5.2.4 an explanation will always be required for payments into or out of client account by or from a third party

6 What are money laundering and terrorist financing?

6.1 Money laundering is the process through which the true origin and ownership of the proceeds of crime are changed so that the proceeds appear legitimate. The money laundering offences that are relevant to our firm and staff are explained at section 8.

6.2 Terrorist financing is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism. The terrorist financing offences that are relevant to our firm and staff are explained at section 10.

6.3 Why are anti-money laundering and counter-terrorist financing important to me?

6.3.1 Lawyers facilitate significant transactions and are gatekeepers to the legal system. The AML and CTF regime is designed to prevent our services being used by criminals.

6.3.2 You have obligations under the AML/CTF regime to spot and report money laundering and terrorist financing. Failure to meet these obligations can lead to criminal penalties, substantial fines, disciplinary action by the SRA and untold damage to your own and the Practices's reputation—see section 8.6.

6.4 How does money get laundered?

6.4.1 Typically, money laundering involves three stages:

(a) **Placement**—the process of placing criminal property into the financial system (eg by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) which are deposited at different locations)

(b) **Layering**—the process of moving money that has been placed in the financial system in order to obscure its criminal origin (usually through multiple complex transactions often involving complicated offshore company structures and trusts)

(c) **Integration**—once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds (involves investing the money in legitimate businesses and other investments such as property purchases, or setting up trusts)

6.4.2 We are most likely to become involved in the layering stage but potentially could be involved in any stage.

7 Money laundering/terrorist financing warning signs

7.1 You do not have to behave like a police officer, but you do have to remain alert to the warning signs of money laundering and terrorist financing and make the sort of enquiries that a reasonable person (with the same qualifications, knowledge and experience as you) would make.

7.2 Typical signs of money laundering and terrorist financing can be broken down into four categories: (i) the client, (ii) the parties, (iii) the instructions and (iv) the money and then further by area of law.

7.2.1 The client—red flags

(a) obstructive or secretive clients;

(b) clients who are using an intermediary, or do not appear to be directing the transaction, or appear to be disguising the real client;

(c) clients who avoid personal contact without good reason;

(d) clients who are reluctant to provide information or documentation, or the documentation provided is suspicious;

(e) corporate clients that you are unable to find online or which use free email domains such as Gmail or Hotmail;

(f) clients who ask repeated questions on the law and procedures relating to our identifying and reporting procedures under the AML and CTF regime;

(g) clients based a long way from us with no apparent reason for instructing us;

(h) clients who have changed their legal advisor a number of times or who have been refused a service by another lawyer;

(i) clients who have provided false or stolen identification documentation or information on establishing a relationship;

(j) clients established in high-risk third countries—which means a country that has been identified by the European Commission (EC) as high-risk and section 20 for further information;

(k) corporate clients with unusual or excessively complex structures;

(l) a long-term client starts making requests that are out of character;

(m) a client repeatedly asking for services outside your or your firm's area of expertise;

(n) a client requesting arrangements that do not make commercial sense;

(o) the client has criminal associations;

(p) the client has an unusual level of knowledge about money laundering processes;

(q) the client does not appear to have a business association with the other parties involved but appears to be connected to them.

7.2.2 The parties—red flags

(a) the parties are established in high-risk third countries—see section 20;

(b) the parties appear to be connected without any apparent business reason;

(c) the nature of the ties between the parties causes doubts as to the real nature of the transaction;

(d) there are multiple appearances of the same parties in transactions over a short period of time;

(e) the age of the parties is unusual, particularly where a party is under the legal age;

(f) there appear to be attempts to disguise the parties;

(g) the person directing the matter is not a formal party to the transaction.

7.2.3 The instructions—red flags

(a) cases or instructions that change unexpectedly or for no logical reason, especially where:

(i) the client has deposited funds with us; or

(ii) the source or destination of funds changes at the last moment;

(iii) the client unexpectedly asks us to send money received into our client account back to its source, to the client or to a third party;

(b) instructions outside our usual range of expertise;

(c) retainers involving high-risk third countries;

(d) loss-making transactions where the loss is avoidable;

(e) complex or unusually large transactions;

(f) unusual patterns of transactions;

(g) transactions with no apparent economic or legal purpose;

(h) instructions for which the client wants to pay us higher fees than the norm;

(i) instructions that are unusual in any way;

(j) abandoned instructions where the client has no concern for the level of our fees;

(k) retainers exclusively relating to keeping documents or other goods or holding deposits;

(l) disputes which are settled too easily;

(m) dealing with money or property either of which you suspect is being transferred to avoid the attention of a trustee in a bankruptcy, HMRC, or a law enforcement agency;

(n) settlements paid in cash, or paid directly between parties, eg where cash is passed directly between sellers and buyers without adequate explanation.

7.2.4 The money—red flags

(a) the client asks you to return funds or send funds to a third party;

(b) money transfers where there is a variation between the account holder and signatory;

(c) payments to or from third parties where there is no logical connection to the client;

(d) large amounts of cash or private funding being used, especially where you are aware that your client has a low income;

(e) large payment on account of fees with instructions terminated shortly after, followed by the client requesting the funds are returned;

(f) movement of funds between accounts, institutions or jurisdictions without reason or to or from a high risk third country;

(g) multiple bank accounts used with no logical explanation;

(h) funding coming from a company, business or government for a private matter;

(i) requests to change payment procedures that are already agreed;

(j) the source of funds is unusual in any way.

Remember: payments made through the mainstream banking system are not guaranteed to be clean.

7.2.5 Litigation—red flags

(a) disputes that settle too easily (consider whether the matter involves sham litigation);

(b) direct payments between the parties;

(c) a third party is providing funding without logical reason.

7.2.6 Private client matters—red flags

(a) estate assets have been earned or are located in foreign jurisdictions;

(b) the deceased was or their business interests were based in a high risk jurisdiction—see section 7.2.1;

(c) the deceased was accused or convicted of a criminal offence, evaded tax or improperly claimed welfare benefits;

(d) you discover or suspect that beneficiaries are not intending to pay the correct amount of tax or are avoiding some other financial charge;

(e) trusts with unusual structures;

(f) trusts based in high-risk jurisdictions, especially those with strict bank secrecy laws;

(g) charities for whom you receive funds in unusual circumstances which may include receiving a large amount of cash;

(h) a donee has completed an improper financial transaction.

7.2.7 Property matters—red flags

(a) back-to-back property transactions;

(b) properties owned by nominee companies or multiple owners;

(c) sudden or unexplained changes in ownership;

(d) signs of mortgage fraud;

(e) mortgages repeatedly repaid significantly prior to an agreed date;

(f) a third party is providing funding without logical reason;

(g) large payments from private funding where the amount does not fit with your knowledge of the client's financial resources;

(h) direct payments between buyer and seller;

(i) an unusual sale price;

(j) the property is located in a high-risk third country.

7.2.8 Company and commercial matters—red flags

(a) creation of complex ownership structures;

(b) company formations in foreign jurisdictions for no apparent reason;

(c) unusual requests to use our client account.

7.3 Criminals are always developing new techniques so this list can never be exhaustive.

7.4 The sort of enquiries you should be making are:

7.4.1 how is the deal being financed: where is the money coming from?

7.4.2 how does the client expect to benefit from the deal/matter?

7.4.3 where are the proceeds of the deal/matter going to—if not to the client, why not?

7.4.4 who are the people behind any company?

7.4.5 who are the parties involved?

7.4.6 does the size of the transaction match your knowledge of the client's finances and typical transaction size?

8 Money laundering offences

8.1 The Proceeds of Crime Act 2002 (POCA 2002) establishes a range of money laundering offences:

8.1.1 the principal offences;

8.1.2 failure to disclose offences; and

8.1.3 the offences of tipping-off and prejudicing an investigation.

8.2 Each offence is explained below. All money laundering offences relate to criminal property, which is property that constitutes or represents a person's benefit:

8.2.1 in whole or in part;

8.2.2 from criminal conduct;

8.2.3 whether directly or indirectly.

8.3 This definition covers the proceeds of all crimes. There is no minimum limit on what is considered to be criminal property.

8.4 Criminal conduct is all conduct that constitutes an offence in any part of the UK or overseas conduct that would constitute a criminal offence in the UK that would attract a maximum sentence of more than 12 months' imprisonment.

8.5 The principal offences

8.5.1 You will commit a principal money laundering offence if you:

(a) conceal, disguise, convert, transfer or remove criminal property from the UK (POCA 2002, s 327);

(b) enter into or become concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property for or on behalf of another (POCA 2002, s 328); or

(c) acquire, use or have possession of criminal property (POCA 2002, s 329).

8.5.2 Concealing (POCA 2002, s 327)

(a) You will commit an offence if you:
  (i) conceal;
  (ii) disguise;
  (iii) convert;
  (iv) transfer; or
  (v) remove from the UK.
  criminal property.

(b) This includes concealing or disguising its:
  (i) nature;
  (ii) source;
  (iii) location;
  (iv) disposition;
  (v) movement; or
  (vi) ownership.

or any rights with respect to it.

(c) You must know or suspect that the criminal property represents a benefit from criminal conduct.

8.5.3 Arrangements (POCA 2002, s 328)

(a) You will commit an offence if you:

(i) enter into or become concerned in;

(ii) an arrangement which you know or suspect facilitates (by whatever means);

(iii) the acquisition, retention, use or control of criminal property;

(iv) by or on behalf of another.

(b) Arrangement is not defined in POCA 2002, though POCA 2002, s 328 catches a wide range of involvement in money laundering offences. It can easily catch you when you are conducting transactional work for laundering clients.

(c) Section 328 will not catch legal professionals conducting genuine litigation or carrying out the terms of a court order. However, any property will remain criminal after litigation has concluded and any resulting court order implemented, so you may decide to advise the client to seek advice in relation to the property from an independent legal professional. For example:

(i) in matrimonial proceedings between husband A (a criminal) and wife B

(ii) the court orders the transfer of the matrimonial home from A to B

(iii) the matrimonial home represents the proceeds of A's crime

(d) You will not commit the arrangement offence by effecting the transfer under the court order. However, the matrimonial home remains criminal property in B's hands. If B later instructs you to transfer the property, you will commit the arrangement offence if you do not first disclose your knowledge about the property and receive appropriate consent, or a defence, from the National Crime Agency (NCA) to transfer it.

(e) Entering into an arrangement means becoming party to it. Being concerned in an arrangement has a wider scope, eg taking steps to put an arrangement in place.

(f) Preparatory or intermediate steps which do not in themselves involve the acquisition, retention, use or control of property will not constitute the making of an arrangement.

8.5.4 Acquisition (POCA 2002, s 329)

(a) You will commit an offence if you:

(i) acquire

(ii) use, or

(iii) have possession of

criminal property.

8.5.5 Possession means having physical custody of the criminal property.

8.5.6 The principal money laundering offences carry a maximum penalty of 14 years' imprisonment, a fine or both.

8.5.7 You will have a defence to a principal money laundering offence if you submit a Suspicious Activity Report (SAR) to the nominated officer.

8.6 Failure to disclose

8.6.1 Making a SAR to the nominated officer can be a defence to a principal money laundering offence.

8.6.2 Failing to make a SAR to the nominated officer where you know or suspect money laundering is an offence in itself which is punishable by up to five years' imprisonment, a fine or both.

8.6.3 See further section 11.

8.7 Tipping-off and prejudicing an investigation

8.7.1 You will commit the tipping-off offence if you:

(a) disclose that you, or anyone else has made a SAR to the nominated officer (or the NCA) of information which came to you in the course of business; and

(b) that disclosure is likely to prejudice any investigation that might be conducted following the SAR.

8.7.2 You will commit the prejudicing an investigation offence if you disclose that an investigation is being contemplated or carried out and that disclosure is likely to prejudice that investigation.

8.7.3 You will also commit an offence if you know or suspect an investigation is being or is about to be conducted and you interfere with documents that are relevant to the investigation.

8.7.4 Tipping-off can only be committed after a SAR (including an internal SAR to the nominated officer) has been made.

8.7.5 You will not commit tipping-off by discussing your concerns with or submitting a SAR to the nominated officer.

8.7.6 All these offences are punishable by up to five years' imprisonment, a fine or both.

8.7.7 The existence of these offences does not prevent you from making normal enquiries about your clients' instructions. You are able to make enquiries in order to:

(a) obtain further information to help you decide whether you have a suspicion; and/or

(b) remove any concerns that you have.

8.7.8 Your enquiries will only constitute an offence if you disclose that a SAR has been made or an investigation is being carried out or contemplated.

8.7.9 It is not tipping-off to warn your clients of your duties under the AML/CTF regime by providing them with our terms of business

8.7.10 Before establishing a business relationship with a company or LLP client we must collect proof of registration or an excerpt of the register (eg the register maintained by Companies House).

8.7.11 If we find a discrepancy between the beneficial ownership information on the register and the information made available to us in the course of carrying out our CDD exercise, we must report it to the registrar.

8.7.12 While it is unlikely that making a discrepancy report to Companies House where required in itself would amount to tipping-off (see section 11.12.1), you must exercise caution where you consider it necessary to submit both a SAR and a discrepancy report. If in doubt, seek advice from the nominated officer.

9 Terrorist financing offences

9.1 Terrorists need funds to plan and carry out attacks. The Terrorism Act 2000 (TA 2000) criminalises both the participation in terrorist activities and terrorist financing.

9.2 In general terms, terrorist financing is:

9.2.1 the provision or collection of funds

9.2.2 from legitimate or illegitimate sources

9.2.3 with the intention or in the knowledge

9.2.4 that they should be used in order to carry out any act of terrorism

9.2.5 whether or not those funds are in fact used for that purpose.

9.3 The TA 2000 establishes a similar pattern of offences to those contained in POCA 2002, ie:

9.3.1 principal terrorism offences of:

(a) fundraising;
(b) use or possession;
(c) arrangements;
(d) money laundering;

9.3.2 failure to disclose offences;

9.3.3 tipping-off offences.

9.4 All offences carry heavy criminal penalties.

9.5 While the terrorist financing and money laundering regimes are different, they share similar aims and structures and run together in UK legislation.

9.6 Many of the provisions of POCA 2002 and TA 2000 mirror one another and the definitions are deliberately matched.

9.7 Both POCA 2002 and TA 2000 run parallel to the Money Laundering Regulations 2017 (MLR 2017), which are explained below.

10 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, (MLR 2017), as amended

10.1 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), SI 2017/692 form part of the UK's overall AML and CTF regime. They came into force on 26 June 2017 and give effect to the Fourth Money Laundering Directive (4MLD). They set administrative requirements which run parallel to the criminal element of the AML and CTF regime contained in the Proceeds of Crime Act 2002 (POCA 2002) and the Terrorism Act 2000 (TA 2000). There is some overlap with this legislation.

In July 2018, the Fifth Money Laundering Directive (5MLD) came into force. It is an 'Amending Directive' because it amends 4MLD. Implementing the requirements of 5MLD involved the UK government making changes to the MLR 2017 through the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, SI 2019/151, in force from 10 January 2020, and from 6 October 2020, the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020, SI 2020/91. Requirements in this Policy reflect the amended MLR 2017.

11 Reporting suspicions

11.1 We have a strict duty to keep the affairs of our clients confidential. The circumstances in which you can disclose information about our clients are very limited.

11.2 However, POCA 2002 and TA 2000 impose obligations to report knowledge or suspicion of money laundering or terrorist financing by way of a SAR. These obligations can override your duty of confidentiality.

11.3 Our internal SAR form can be found at Appendix 1.

11.4 Any member of staff can submit a SAR form to the nominated officer.

11.5 What are knowledge and suspicion?

11.5.1 'Knowledge' under POCA 2002 means actual knowledge.

11.5.2 'Suspicion' is a possibility which is more than fanciful. A vague feeling of unease will not suffice.

11.5.3 There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a belief which is beyond mere speculation.

11.5.4 The test for whether you hold a suspicion is generally subjective. However, there is an objective element to the test, ie would the reasonable solicitor, with the same knowledge, experience and information, have formed a suspicion.

11.5.5 The suspicion held must be that another person is engaged in money laundering and not simply that there is something 'fishy' about the client or the transaction.

11.6 When should I report suspicions?

11.6.1 ALWAYS and as soon as reasonably practicable.

11.6.2 If you know or suspect that another person is engaged in money laundering or terrorist financing you must complete the SAR form (see Appendix 1) and send it to

the nominated officer. Our nominated officer is Andrew Flagg. In their absence, SAR forms must be sent to our COLP Grant Sanders.

11.7 How do I make a report?

11.7.1 If you know or suspect that your matter involves money laundering or terrorist financing you must complete the SAR form, see Appendix 1.

11.7.2 The person nominated to receive internal SAR forms is Andrew Flagg or, in their absence, Grant Sanders.

11.7.3 If you require consent to continue with the matter then you must indicate this by using the relevant box on the SAR form. You will only receive consent to the extent that you ask for it so remember to include every step that you will need to take to complete the matter on the SAR form.

11.7.4 You must make your report as soon as reasonably practicable. You will be required to explain any delays to the nominated officer.

11.7.5 **Do not** keep a copy of the SAR form on the client file.

11.8 What should I do if I am unsure why I am suspicious?

11.8.1 If you are unsure whether you suspect money laundering or terrorist financing, eg something just does not feel right with the matter, do not complete the SAR form but discuss your concerns with the nominated officer, who will advise whether you need to submit a SAR form. We will keep a note of that discussion.

11.9 Does legal professional privilege apply?

11.9.1 Legal professional privilege may be a defence to a failure to report offence. It is a hugely complex area of law.

11.9.2 You should make a SAR to the nominated officer even where you believe privilege may apply. It is for the nominated officer to decide whether privilege applies and to what extent it affects our reporting obligations under POCA 2002 and TA 2000.

11.10 What happens after I make a SAR?

11.10.1 On receiving your SAR form, the nominated officer will consider the reasons for suspicion reported to them. They may ask you for more information.

11.10.2 The nominated officer will then decide whether an external SAR to the NCA is required. This decision rests only with the nominated officer, or their deputy in their absence.

11.10.3 You have discharged your reporting obligations under POCA 2002 and TA 2000 by making the internal SAR.

11.10.4 If you need consent or a defence to continue acting for the client where to do so will involve your committing a principal offence, you must indicate this on the SAR form. The nominated officer will refer to the NCA for its consent/a defence.

11.10.5 The NCA has seven working days following receipt of a SAR to decide whether to give consent. If within this period the NCA gives consent, or does not refuse consent, you will have a defence to a principal money laundering or terrorist financing offence. This means that you can continue to act and take steps which would otherwise constitute an offence within the limits of the consent requested.

11.10.6 If the NCA refuses consent within seven working days of receiving the SAR, it has a further 31 days to take action. If we hear nothing within this period from the NCA we will be deemed to have its consent which means that, strictly, we can continue to act. But we must remain alert to the possible ethical and reputational consequences of so doing.

11.10.7 In exceptional circumstances the NCA may apply to the court to extend the moratorium period for further 31 day periods, up to a maximum of 186 days over the original 31 days.

11.10.8 You must follow instructions from the nominated officer during the period set out in section 11.10.5 and/or 11.10.6. You may work on the matter in the meantime but **must not:**

(a) transfer funds;

(b) take an irrevocable step in the matter (eg sign contracts or complete a deal); or

(c) do anything that constitutes tipping off—see section 11.11.

11.10.9 You can take steps which do not amount to committing a principal offence, such as writing letters or conducting searches.

11.10.10 If in doubt, seek guidance from the nominated officer.

11.11 What can I tell the client?

11.11.1 You **must not** tell the client that you have submitted a SAR. If you do you will be committing the offence of tipping-off and could be exposed to a criminal record and up to five years' imprisonment.

11.11.2 There is very little, if anything, that you can tell the client after you have submitted a SAR.

11.11.3 Always speak with the nominated officer if you are in any doubt.

11.12 SARs and beneficial ownership discrepancies

11.12.1 Reporting a discrepancy in relation to beneficial ownership information to Companies House (see section 32) is not the same as submitting a SAR.

11.12.2 If you suspect money laundering or terrorist financing in a situation where you have submitted or plan to submit a discrepancy report form, you must also submit a SAR.

11.13 SuperSARs

11.13.1 SuperSARs are SARs compiled by more than one regulated organisation which are then submitted jointly to the NCA. They are designed to reduce the number of SARs the NCA receives by allowing private sector entities to share information about

suspected money laundering or terrorist financing before providing this information to the NCA in a single SAR.

11.13.2 If you receive a request or notification from the NCA or another regulated organisation relating to a superSAR, you must inform the nominated officer immediately.

12 CDD–what is client due diligence?

12.1 Client due diligence is usually referred to as CDD. There are three basic components of CDD:

12.1.1 identifying and verifying the client's identity

12.1.2 identifying the beneficial owner where this is not the client

12.1.3 obtaining details of the purpose and intended nature of the business relationship

12.2 We are also required to conduct ongoing monitoring of business relationships with our clients.

12.3 There are three levels of CDD:

12.3.1 simplified due diligence (SDD)

12.3.2 enhanced due diligence (EDD)

12.3.3 regular due diligence (RDD)

12.4 All levels of CDD require you to identify and verify your client, but each level has different identification and verification requirements. These are set out in section 16.6 and in our CDD matrix at Appendix 2.

12.5 CDD also requires us to identify and validate the identity of beneficial owners of a client.

13 CDD—who is the client?

13.1 In general, the client will be the party, or parties, with whom the firm is establishing a business relationship, or for whom the transaction is carried out.

13.2 Things can become more complicated with beneficial owners or where someone is acting on behalf of the client.

13.3 Ownership, control and beneficial owners

13.3.1 Where the client is a legal person, trust, company, foundation or similar legal arrangement we must take reasonable measures to understand the ownership and control structure of that client.

13.3.2 Where the client is beneficially owned by another person, we must:

(a) identify the beneficial owner, ie the natural person(s) who ultimately owns or controls the client, and/or the person on whose behalf a transaction is being conducted

(b) take reasonable measures to verify the identity of the beneficial owner so that you are satisfied that you know who the beneficial owner is, and

(c) if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement, take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement

13.3.3 See further section 26.

13.4 Person acting on the client's behalf

13.4.1 The concept of beneficial ownership should not be confused with a situation where a client appoints someone to act on their behalf. Where a person (the representative) purports to act on behalf of the client we must:

(a) verify that the representative is authorised to act on the client's behalf

(b) identify the representative, and

(c) verify the identity of the representative on the basis of documents or information obtained from a reliable source which is independent of both the representative and the client

13.4.2 For the specific measures you must take, please refer to our CDD risk matrix at Appendix 2.

14 CDD—in which situations is CDD required?

14.1 Standard CDD triggers

You must apply CDD measures:

14.1.1 when you establish a business relationship with a client;

14.1.2 when you carry out an occasional transaction for a client;

14.1.3 when you suspect money laundering or terrorist financing;

14.1.4 when you doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification;

14.1.5 where the client has not been in regular contact with us for one year or more;

14.1.6 in relation to existing clients as set out at section 14.2.

14.2 CDD on existing clients

14.2.1 There is no provision in the Regulations for waiving CDD requirements on the basis of long-standing or personal relationships. Taking this approach will not satisfy the requirement to undertake independent verification, though these factors may inform your risk-based approach.

14.2.2 You must apply CDD measures at appropriate times to existing clients on a risk-sensitive basis, and if you become aware that the circumstances of an existing client have changed in a way that is relevant to your assessment of risk for that client.

14.2.3 In determining when it is appropriate to conduct CDD on existing clients, you must take into account, among other things:

(a) any indication that the identity of the client (or its beneficial owner) has changed;

(b) any transactions which are not reasonably consistent with your knowledge of the client;

(c) any change in the purpose or intended nature of your relationship with the client; and

(d) a gap in the retainer of three years or more;

(e) a client instructing on a high-risk matter;

(f) an existing high-risk client;

(g) any legal duty you have in the course of the calendar year to contact an existing client for the purpose of reviewing any information which is relevant to your risk assessment for that client, and relates to the beneficial ownership of the client, including information which enables you to understand the ownership or control structure of a legal person, trust, foundation or similar arrangement who is the beneficial owner of the client

(h) in order to fulfil any duty under the International Tax Compliance Regulations 2015

(i) any other matter which might affect your assessment of the money laundering or terrorist financing risk in relation to that client.

14.2.4 If you are in any doubt please contact the nominated officer.

15 CDD—in what time frame must CDD be completed?

15.1 The timing of our CDD exercise depends on the nature of the client relationship:

Occasional transaction—timing of CDD	**Business relationship—timing of CDD**
Before you carry out the occasional transaction	Before you establish a business relationship, or as soon as possible after initial contact during the establishment of the relationship where: —this is necessary so as not to interrupt the normal conduct of business, and —there is little risk of money laundering

15.2 In either case, you must not transfer funds or property or permit final arrangements to be signed before verification is complete.

15.3 You must seek guidance from the nominated officer if there is any delay in the CDD process. They will advise on steps to take and, where necessary, consider whether any delay in completing the CDD process is in itself grounds to suspect money laundering or terrorist financing.

16 CDD process

16.1 CDD is a central pillar of the AML and CTF regime. CDD requirements underpin the MLR 2017.

16.2 The component parts of CDD are:

16.2.1 identifying a client

16.2.2 verifying that identity on the basis of documents or information obtained from a reliable source which is independent of the client, and

16.2.3 assessing, and where appropriate obtaining information on, the purpose and intended nature of the business relationship or transaction

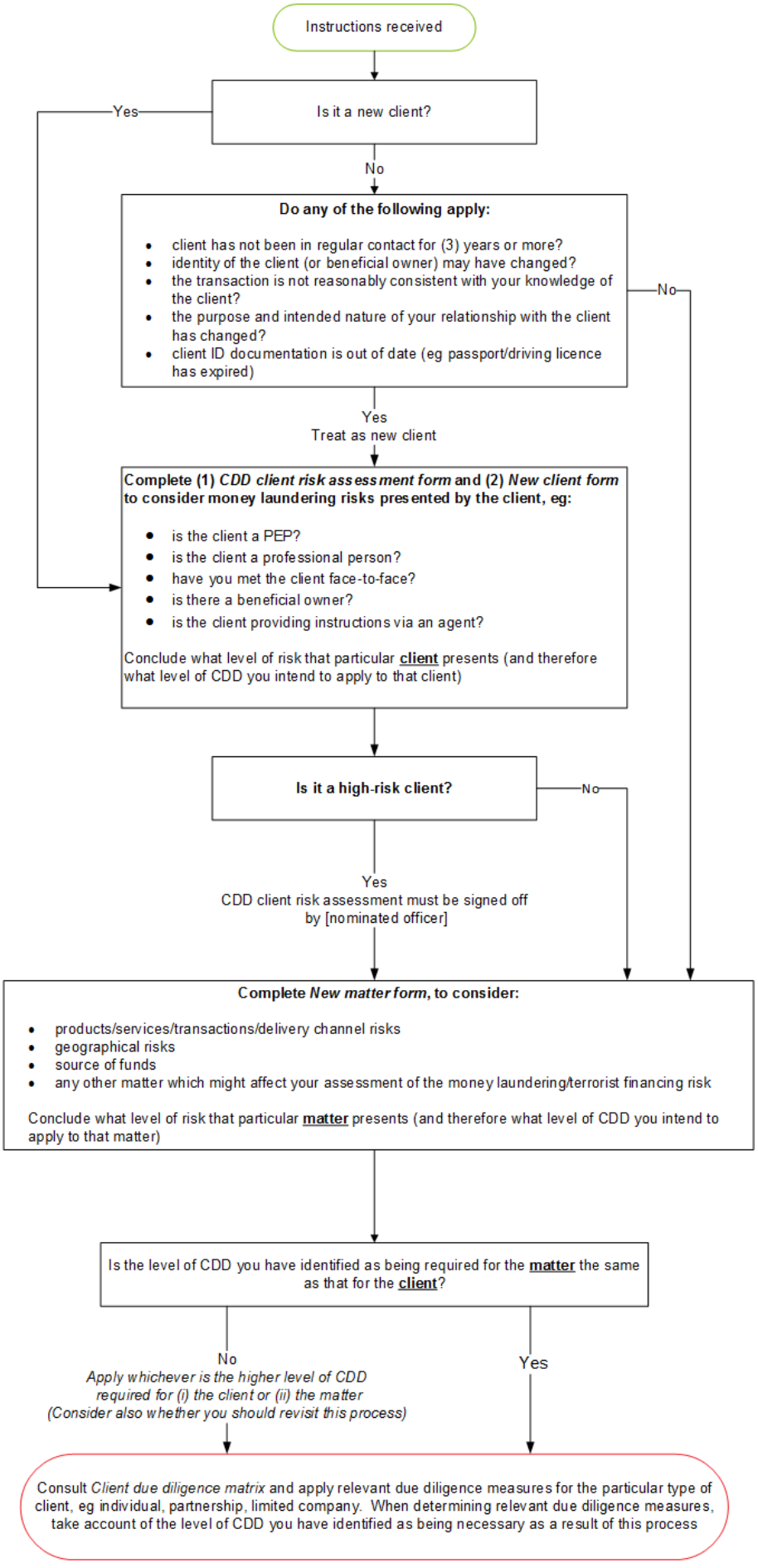
16.3 We must determine the extent of our CDD measures on a risk-sensitive basis, depending on the type of client, business relationship and matter. We must also be able to demonstrate to our regulatory body that the extent of our CDD measures are appropriate in view of the risks of money laundering and terrorist financing:

16.3.1 identified in our firm–wide risk assessment, and

16.3.2 as identified by our supervisory authority and made available to us

16.4 The following flowchart sets out our process for conducting CDD, starting with risk assessment:

16.5 PLEASE NOTE FOR SDD AND EDD ALL DOCUMENTS MUUST BE SAVED UNDER THE CLIENT TAB ON THE CASE MANAGEMENT SYSTEM


Instructions received
Is it a new client?
Yes
No
Do any of the following apply:
client has not been in regular contact for (3) years or more?
identity of the client (or beneficial owner) may have changed?
the transaction is not reasonably consistent with your knowledge of the client?
the purpose and intended nature of your relationship with the client has changed?
client ID documentation is out of date (eg passport/driving licence has expired)
No
Yes
Treat as new client
Complete (1) CDD client risk assessment form and (2) New client form to consider money laundering risks presented by the client, eg:
is the client a PEP?
is the client a professional person?
have you met the client face-to-face?
is there a beneficial owner?
is the client providing instructions via an agent?
Conclude what level of risk that particular client presents (and therefore what level of CDD you intend to apply to that client)
Is it a high-risk client?
No
Yes
CDD client risk assessment must be signed off by [nominated officer]
Complete New matter form, to consider:
products/services/transactions/delivery channel risks
geographical risks
source of funds
any other matter which might affect your assessment of the money laundering/terrorist financing risk
Conclude what level of risk that particular matter presents (and therefore what level of CDD you intend to apply to that matter)
Is the level of CDD you have identified as being required for the matter the same as that for the client?
No
Apply whichever is the higher level of CDD required for (i) the client or (ii) the matter
(Consider also whether you should revisit this process)
Yes
Consult Client due diligence matrix and apply relevant due diligence measures for the particular type of client, eg individual, partnership, limited company. When determining relevant due diligence measures, take account of the level of CDD you have identified as being necessary as a result of this process

16.6 Client and matter risk assessment

16.6.1 You must start by assessing the risk of money laundering or terrorist financing posed by the specific client and complete the CDD client electronic risk assessment form. Once this is complete you must decide what level of CDD is necessary in terms of the client itself. This will inform your next steps.

16.6.2 Despite the term 'client' due diligence, CDD doesn't just relate to the client itself. The MLR 2017 also require us to consider the risks associated with the business relationship, which is broader than just the client, including:

(a) product, service, transaction or delivery channel risks;

(b) geographical risk factors (which may apply to the client or to the matter/transaction itself).

16.6.3 We also consider the elevated risks attached to certain sectors which have been identified by credible sources as giving rise to an increased risk of corruption, eg:

(a) Domestic and international public work contracts and construction, including post-conflict reconstruction;

(b) real estate and property development;

(c) the oil and gas industry (with the exception of the buying and selling of fuel for domestic consumption or retail);

(d) aspects of the nuclear industry with vulnerability to proliferation risk;

(e) mining (including precious metals, diamond or other gemstones and trading of these materials);

(f) arms manufacturing/supply and the defence industry

(g) businesses utilising new or unproven technology, that might make them vulnerable to being used for money laundering;

(h) high value goods businesses;

(i) items of archaeological, historical, cultural and religious significance or of rare scientific value (this may be of particularly high risk in jurisdictions with exposure to terrorism or terrorist financing activities);

(j) tobacco products;

(k) gambling;

(l) crypto-asset wallet providers and exchanges;

(m) unregulated charities (particularly those operating in higher risk jurisdictions);

(n) money transfer businesses;

(o) ivory and other items and materials related to protected species

16.6.4 Matter risk assessment is a key part of our AML/CTF measures. It is an ongoing process; information gathered in the course of acting for a client will inform the risk assessment process. Our Anti-money Laundering and Transactional Risk Assessments require you to consider the AML/CTF risk of the matter at the outset. If there is any change to the nature of the risk throughout the course of the matter, you must record that fact, as well as any actions taken as a result, on the file information sheet and inform the nominated officer as appropriate.

16.6.5 Unless section 14.2 applies, we do not conduct the full CDD process for each new matter we open for an existing client. It is therefore important to get as full a picture as possible when we take on a new client and decide on the correct level of CDD at

the outset of our relationship with each new client. When an existing client instructs us on a new matter, we should look at the instructions we typically receive and the type of work we're doing for that client before applying CDD measures. If the type of work or instructions change, you will need to start again from the beginning and re-assess the risk presented by the business relationship with that client. See further sections 14.2 and 28.

16.6.6 Our CDD matrix at Appendix 2, contains information on risk assessment and CDD measures for various types of client which must be followed in every case. This will help you to complete your CDD electronic risk assessment form.

16.7 Required documentation

16.7.1 Once you have completed your risk assessment, you will be able to decide what level of CDD to apply, ie EDD, SDD or RDD.

16.7.2 The specific CDD measures you must then apply and the documents you must obtain in each case are set out in our CDD matrix at Appendix 2.

16.7.3 It is your responsibility to check the accuracy and adequacy of the documents provided.

16.7.4 If you are in any doubt please contact the nominated officer immediately.

16.8 Clients who cannot provide the standard documents

16.8.1 Sometimes clients are unable to provide standard verification documents.

16.8.2 In these circumstances we will consider whether the inability to provide us with standard verification is consistent with the client's profile and circumstances or whether it might make us suspicious that money laundering or terrorist financing is occurring.

16.8.3 Where we decide that a client has a good reason for not meeting the standard verification requirements, we will consider accepting other forms of documentation, eg:

Client type	Acceptable documentation
Client in care home	A letter from the manager
Client without a permanent residence	A letter from a householder named on a current council tax bill or a hostel manager, confirming temporary residence
Refugee	A letter from the Home Office confirming refugee status and granting permission to work, or a Home Office travel document for refugees
Asylum seeker	Registration card and any other identity documentation they hold, or a letter of assurance as to identity from a community member such as a priest, GP, or local councillor who has knowledge of the client

Client type	Acceptable documentation
Student or minor	A birth certificate and confirmation of their parent's address or confirmation of address from the register of the school or higher education
Person with mental health problems or mental incapacity	Confirmation of identity from medical workers, hostel staff, social workers, deputies or guardians appointed by the court

17 CDD records

17.1 We also have an obligation to keep documents, data or information used for the purposes of applying CDD measures up to date. Our system to record when CDD records (eg passports) are due to expire so you can obtain the updated version or alternative documentation involves setting flags within our case management system.

17.2 We are obliged to keep the following records:

17.2.1 a copy of CDD records, including:

(a) appropriate data identifying and verifying the client's name, company number, address, board members/directors and beneficial owner;

(b) appropriate data identifying and verifying the identity of any person who purports to act on behalf of a client;

(c) appropriate data required and obtained under EDD processes;

(d) where we are unable to identify the beneficial owner and so treat the senior person in the company as its beneficial owner (see section 26.6), written records of all the actions we have taken to identify the beneficial owner, all the actions we have taken to identify and verify the identity of the senior person and any difficulties we encountered in doing so;

17.2.2 sufficient supporting records (originals or copies) in respect of a matter to enable the transaction/matter to be reconstructed.

18 CDD—different levels of CDD

There are three levels of CDD: simplified, enhanced and regular.

18.1 Simplified due diligence (SDD)

18.1.1 SDD is not an exemption from CDD; it is simply a downwards adjustment of the level of measures you take to comply with CDD requirements. The information you obtain when applying SDD measures must enable us to be reasonably satisfied that the risk associated with the relationship is low and be sufficient to give us enough information about the nature of the business relationship to identify any unusual or suspicious transactions.

18.1.2 We can apply SDD in relation to particular business relationships or transactions which we determine present a low risk of money laundering or terrorist financing, having taken into account:

(a) our firm-wide risk assessment

(b) relevant information provided by our supervisory authority, and

(c) specified risk factors set out in the MLR 2017—these are incorporated into our client and matter inception procedures

18.1.3 SDD is also not an exemption from reporting suspicious activity to the nominated officer—see section 11.

18.1.4 Bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering or terrorist financing in a particular situation, but it is important that we consider all these risk factors for every client.

19 Enhanced due diligence

19.1 EDD is a higher level of CDD, required to mitigate the increased risk presented by certain clients and certain situations.

19.2 We must apply EDD measures and enhanced ongoing monitoring:

19.2.1 in any case identified as presenting a high risk of money laundering or terrorist financing in our firm-wide risk assessment or by our supervisory authority;

19.2.2 in any transaction or business relationship with a person established in a high-risk third country—see section 20;

19.2.3 where the client/potential client is a politically exposed person (PEP), or a family member or known close associate of a PEP—see section 21;

19.2.4 where a client has provided false or stolen identification documentation or information for CDD purposes;

19.2.5 for non-face-to-face business relationships/transactions;

19.2.6 in any case where:

(a) a transaction is complex or unusually large;

(b) there is an unusual pattern of transactions; or

(c) the transaction or transactions have no apparent economic or legal purpose—see section 22;

19.2.7 in any other case which by its nature can present a higher risk of money laundering and terrorist financing, taking into account various specified risk factors set out in the MLR 2017, eg matters favouring anonymity, see section 19.2.8.

19.2.8 matters favouring anonymity, including, eg those involving opaque trust or company structures, overly complex matters (eg obscuring parties or source of funds), transactions involving cash, electronic currency or virtual assets, non-face-to-face clients, services where we act as trustee/director that allows the client's identity to remain anonymous, matters for clients who are celebrities and wish to remain anonymous, or clients which are evasive as to the identity of the parties involved. The exact measures we take for these matters will depend on the circumstances, but include at least those set out in section23.

Bear in mind that the presence of one or more risk factors may not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation, but it is important that we consider all these risk factors for every client.

20 CDD—high-risk third countries

20.1 We must apply EDD measures and enhanced ongoing monitoring in any business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high risk third country.

20.2 What is a high-risk third country?

20.2.1 A high-risk third country means a country which has been identified by the European Commission in delegated acts adopted under Article 9.2 of the 4MLD as a high-risk third country.

20.2.2 The requirement to apply EDD for high-risk third countries applies where there is a relevant transaction and establishment in a high-risk third country. A relevant transaction is a transaction in relation to which you are required to apply customer due diligence (CDD) measures under regulation 27, MLR 2017, and being established in a country means:

(a) in the case of a legal person, being incorporated in or having its principal place of business in that country, or, in the case of a financial institution or a credit institution, having its principal regulatory authority in that country; and

(b) in the case of an individual, being resident in that country, but not merely having been born in that country.

20.2.3 You are not required to apply EDD where the client is a branch or majority-owned subsidiary undertaking of an entity which is established in an EEA state if all of the following conditions are satisfied:

(a) the entity is subject to the requirements in national legislation implementing 4MLD as an obliged entity, and supervised for compliance with those requirements;

(b) the branch or subsidiary complies fully with procedures and policies established for the group; and

(c) having applied a risk-based approach, you do not consider that it is necessary to apply EDD measures.

20.2.4 We maintain a list of high-risk third countries, which you can find within the electronic Risk Assessment.

20.2.5 Note that countries not specifically identified by the European Commission are not automatically considered to have effective AML and CTF systems. If in doubt, contact the nominated officer.

20.3 EDD measures for matters involving high-risk third countries

20.3.1 EDD measures for matters involving high-risk third countries must include:

(a) obtaining additional information on the client and on the client's beneficial owner—see section 26;

(b) obtaining additional information on the intended nature of the business relationship—see section 28;

(c) obtaining information on the source of funds and source of wealth of the client and of the client's beneficial owner—see section 27;

(d) obtaining information on the reasons for the transactions—see section 28;

(e) obtaining the approval of senior management for establishing or continuing the business relationship—see section 24

(f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination—see section 33.

21 CDD—politically exposed persons (PEPs)

21.1 Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher money laundering risk as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities, but it does put the client or the beneficial owner into a higher risk category.

21.2 What is a PEP?

21.2.1 A PEP is an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official, including:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of any other judicial body the decisions of which are not subject to further appeal except in exceptional circumstance;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, charges d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of state-owned enterprises; and

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

21.2.2 Our arrangements for PEPs extend to family members and known close associates of PEPs:

Family members	Known close associates
Spouse or partner Children of that person and their spouses or partners Parents of that person	An individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a PEP An individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP

21.3 How we identify PEPs

21.3.1 Establishing whether individuals qualify as PEPs is not always straightforward and can present difficulties.

21.3.2 To determine whether a client or its beneficial owner is a PEP or a family member or known close associate of a PEP, and to manage the enhanced risks arising from our relationship with such a client, we use an automated PEP screening service within our electronic checks.

21.3.3 It is important that we all remain alert to situations suggesting the client is a PEP, eg:

(a) receiving funds from a government account;

(b) correspondence on official letterhead paper from the client or a related person;

(c) general conversation with the client or person related to the retainer linking the person to a PEP; or

(d) news reports coming to your attention suggesting your client is a PEP, or is linked to one.

21.3.4 Once we have established that a client is a PEP, we must apply EDD measures to that client—see section 21.4.

21.4 EDD measures for PEPs

21.4.1 The EDD measures we take for PEPs depend on the level of risk associated with the particular client. Of course all PEPs must be treated as high-risk, but some will be higher risk than others.

21.4.2 Relevant factors to consider include:

(a) the particular circumstances of the PEP;

(b) the PEP's separate business interests and the time those interests prevailed in relation to the public position;

(c) whether the PEP has access to official funds, makes decisions regarding the allocation of public funds or public procurement contracts;

(d) the PEP's home country;

(e) the type of activity about which the PEP is instructing you;

(f) whether the PEP is domestic or international, particularly having regard to the services asked for; and

(g) the scrutiny to which the PEP is under in the PEP's home country.

21.4.3 If a PEP is otherwise involved with a client, then you should consider the nature of the risk in light of all relevant circumstances, eg:

(a) the nature of the relationship between the client and the PEP;

(b) the nature of the client (eg where it is a public listed company or regulated entity which is subject to and regulated for AML/CFT requirements, including being subject to reporting obligations, that will be a relevant factor);

(c) the nature of the services sought, eg lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate

consideration, whereas higher risks may exist where we are involved in the movement or transfer of funds/assets, or the purchase of high value property or assets.

21.4.4 For all PEP clients we must:

(a) have approval from senior management for establishing or continuing the business relationship with that person—see section 24;

(b) take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship or transaction—see section 27 and our Source of funds statement at Appendix 3;

(c) conduct enhanced ongoing monitoring of the business relationship with that person—see section 33.

21.4.5 We will also consider applying some or all of the further measures described at section 23.

22 EDD—complex or unusual instructions

22.1 We must apply EDD where:

22.1.1 a transaction is complex or unusually large;

22.1.2 there is an unusual pattern of transactions; or

22.1.3 the transaction or transactions have no apparent economic or legal purpose.

22.2 Whether a transaction is complex or unusually large should be judged in relation to the normal activity of both the firm and the client.

22.3 EDD measures we must apply here include:

22.3.1 as far as reasonably possible, examining the background and purpose of the transaction—see section 28; and

22.3.2 increasing the degree and nature of monitoring of the business relationship to determine whether the transaction or relationship appear to be suspicious—see section 33.

23 EDD measures for other high-risk clients

23.1 Practical steps include:

23.1.1 seeking additional independent, reliable sources to verify information provided by the client;

23.1.2 taking additional measures to understand better the background, ownership and financial situation of the client and other parties to the transaction;

23.1.3 taking further steps to be satisfied that the matter is consistent with the purpose and intended nature of the business relationship;

23.1.4 increasing the monitoring of the business relationship, including greater scrutiny of transactions.

23.2 We will also consider:

23.2.1 increasing the quantity of information obtained for CDD purposes, eg information about the client's or beneficial owner's identity or the client's ownership and control structure, by obtaining and assessing information about the reputation of the client/beneficial owner(s) and assessing any negative allegations against them, information about family members and close business partners, information about the client or beneficial owner's past and present business activities, adverse media searches and about the intended nature of the business relationship, eg on the likely size and frequency of current and future matters;

23.2.2 requesting evidence on why the client is looking to instruct you on a specific service, in particular where it is unclear why the client's needs cannot be met better in another way or in a different jurisdiction, and the destination of funds;

23.2.3 requiring the first payment to be carried out through an account verifiably in the client's name and with a bank subject to UK CDD standards;

23.2.4 establishing that the client's source of wealth and the source of funds to be used in the business relationship are (i) not the proceeds from criminal activity, and (ii) consistent with the firm's knowledge of the client and the nature of the business relationship;

23.2.5 verifying the source of wealth and the source of funds, eg by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports;

23.2.6 increasing the frequency of reviews of the business relationship, to ascertain whether the client's risk profile has changed and whether the risk remains manageable;

23.2.7 securing the approval of senior management to commence or continue the business relationship to ensure senior management are aware of the risk the firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk—see section 24.

24 Senior management approval

Where senior management approval is required you must submit your request to the Nominated Officer for approval. Their signature constitutes confirmation that the client/matter can be accepted.

25 Regular due diligence (RDD)

25.1 RDD applies where SDD and EDD do not.

25.2 Details of what RDD looks like in practical terms, including the specific documentary evidence we require, can be found in our CDD matrix at Appendix 2 and our CDD electronic client risk assessment form.

26 CDD—beneficial owners

26.1 CDD on beneficial owners is different to CDD on clients.

26.2 Where the client is a legal person, trust, company, foundation or similar legal arrangement, you must take reasonable measures to understand the ownership and control structure of that client.

26.3 Where the client is beneficially owned by another person, you must:

26.3.1 identify the beneficial owner, ie the natural person(s) who ultimately owns or controls the client, and/or the person on whose behalf a transaction is being conducted;

26.3.2 take reasonable measures to verify the identity of the beneficial owner so that you are satisfied that you know who the beneficial owner is; and

26.3.3 if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement, take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement.

26.4 What is a beneficial owner?

26.4.1 If the beneficial owner of a client is in turn a company you will need to establish the human being at the top of the corporate tree.

26.5 What CDD is required?

26.5.1 For all company, unregistered company, LLP or eligible Scottish partnership clients, we must obtain proof of the client entity's registration or an excerpt of the register (ie Companies House register) from the company, unregistered company or LLP or registrar (in the case of an eligible Scottish partnerships). If you find any discrepancy between the beneficial ownership information on the register and the information made available to you in the course of carrying out CDD, you must report it—see further section 32.

26.5.2 You must then consider the client's risk profile, the structure of the business and the nature of the transaction. This will help you to decide what steps you need to take to verify the beneficial owner's identity. In assessing the risk, you should consider:

(a) why your client is acting on behalf of someone else;

(b) how well you know your client;

(c) the type of business structure and its location;

(d) the nature and risk profile of the matter.

26.5.3 The key is to understand the ownership and control of the client.

26.5.4 To identify the beneficial owner, you must obtain at least their name and record any other identifying details which are readily available, including records which are publicly available, asking your client for the relevant information or using other sources. You will need to assess which identity verification measures are needed, considering the client's risk profile, any business structures involved and the proposed transaction.

26.5.5 The level of verification required will depend on your assessment of your client's risk profile.

26.5.6 Appropriate measures may include:

(a) a certificate from your client confirming the identity of the beneficial owner

(b) a copy of the trust deed, partnership agreement or other such document

(c) shareholder details from an online registry

(d) the passport of, or electronic verification on, the individual

(e) other reliable, publicly available information

26.6 What if I can't identify the beneficial owner?

26.6.1 There may be rare occasions where we are not able to identify the beneficial owner.

26.6.2 The MLR 2017 allow us to treat the senior person responsible for managing the client as its beneficial owner if (and only if) we have exhausted all possible means of identifying the beneficial owner, and:

(a) have not succeeded in doing so, or

(b) we are not satisfied the individual identified is in fact the beneficial owner

26.6.3 Where we treat the senior person as the beneficial owner, we must:

(a) keep written records of all the actions you have taken to identify the beneficial owner; and

(b) take reasonable measures to verify the identity of the senior person in the body corporate responsible for managing it, and keep written records of all the actions you have taken in doing so, and any difficulties you have encountered in doing so.

27 CDD—source of funds

27.1 Understanding our client's source of funds is an important step in the CDD process; the source of funds and the source of wealth are relevant to determining a client's risk profile.

27.2 When am I required to look into the source of funds in a transaction?

27.2.1 You are not required to interrogate all clients about their entire financial history, but you are required to take additional steps to ensure that the transaction is consistent with your knowledge of the client.

27.2.2 You must establish the source of funds involved in a transaction:

(a) in relation to ongoing monitoring—see further section 33;

(b) when conducting CDD on PEPs, including family members and known close associates—see section 21.4; and

(c) when conducting CDD in relation to any business relationship with a person established in a high-risk third country or any relevant transaction where either of the parties to the transaction is established in a high-risk third country—see section 20.

Ongoing monitoring	You must establish the source of funds where necessary as part of your ongoing monitoring of a business relationship.
Conducting CDD on PEPs, family	You must always take adequate measures to

members and known close associates	establish: —the source of funds; and —source of wealth.
Business relationship with a person established in a high-risk third country or relevant transaction where either of the parties to the transaction is established in a high-risk third country	You must obtain information on the source of funds and source of wealth of the client and of the client's beneficial owner.

27.3 What steps should I take?

27.3.1 Scrutinising the source of funds is more than asking for the money to come from a bank account in the clients' name. Your focus should be on understanding how the client can legitimately fund the transaction.

27.3.2 For transactions involving PEPs you should consider whether there:

(a) are any warning signs of corruption; or

(b) is any evidence that government or state funds are being used inappropriately.

27.3.3 Where a third party is providing funding to your client you may need to establish the source of funds. See section 34.3.

27.3.4 You must document your investigations into the source of funds, including any questions asked, responses received and supporting evidence provided.

27.3.5 If you have any concerns about the source of funds you must consider whether you need to submit a SAR to the nominated officer.

28 CDD—purpose and intended nature of the business relationship

28.1 Understanding and, where appropriate, obtaining information on, the purpose and intended nature of the business relationship is the final component of CDD.

28.2 We record details of the purpose and intended nature of a client relationship on our New client form.

28.3 Knowing more about the client and their normal activities will help you to spot something unusual—a transaction which appears to serve no purpose could be a money laundering or terrorist financing warning flag.

29 What happens if I cannot conclude the CDD exercise?

29.1 Where we are unable to conclude the CDD exercise we must:

29.1.1 not carry out a transaction through a bank account with the client or on their behalf;

29.1.2 not establish a business relationship or carry out an occasional transaction with the client;

29.1.3 terminate any existing business relationship with the client;

29.1.4 not accept or return funds from the client or on the client's behalf; and

29.1.5 consider whether a SAR is required.

29.2 There are very limited circumstances in which this may not apply. If you believe the client you are dealing with may fall within an exception to this rule, please contact the nominated officer. You must never unilaterally decide that it is acceptable to delay completion of CDD. If you are unable to apply or complete CDD on any matter, you should immediately seek advice from the nominated officer.

29.3 See section 26.6 for steps to take where you are unable to identify the beneficial owner of a client.

30 CDD—relying on a third party to conduct CDD

30.1 The MLR 2017 allow us to rely on a third party to apply any or all of the required CDD measures, however:

30.1.1 they are very specific about exactly who we can and cannot rely on;

30.1.2 we remain liable for any failure in the third parties application of those measures;

30.1.3 we are required to obtain from the third party all the information needed to satisfy CDD requirements and enter into written arrangements with that third party which enable us to obtain copies of any relevant documents and require the third party to retain those documents;

30.2 Because of the strict regulatory rules around reliance, you must not unilaterally decide to rely on CDD conducted by a third party. You must contact the nominated officer who will decide whether we can rely on the third party and, if so, will provide guidance on the procedure to be followed.

31 CDD—reliance on our CDD by another firm

31.1 We can be relied on by other firms to perform CDD measures on a mutual client.

31.2 Offering or agreeing to confirm that we have carried out appropriate CDD measures in respect of a client is a serious matter. Any such requests from other firms must be forwarded immediately to the nominated officer.

32 Reporting discrepancies in CDD information

32.1 Before establishing a business relationship with a company, unregistered company LLP or eligible Scottish partnership client we must collect proof of registration or an excerpt of the register from the company, unregistered company, LLP or eligible Scottish partnership.

32.2 If we find a discrepancy between the beneficial ownership information on the register and the information made available to us in the course of carrying out our CDD exercise, when establishing a business relationship with a client, we must report it to the registrar (eg Companies House), which must then take appropriate action to investigate it in a timely manner.

32.3 Discrepancies may relate to:

32.3.1 a person listed as a person with significant control (PSC);

32.3.2 a missing PSC;

32.3.3 a PSC exemption;

32.3.4 a PSC type;

32.3.5 an address;

32.3.6 a place of registration;

32.3.7 a date of birth;

32.3.8 a legal form;

32.3.9 a company statement;

32.4 It is not a discrepancy if we hold information that goes beyond or is of a different nature from that required for the register.

32.5 We are not required to actively seek out discrepancies or report information which is subject to legal professional privilege.

32.6 If you discover a discrepancy, you must tell the nominated officer, who will then review the information/documentation and make a report to the relevant registrar.

33 CDD—ongoing monitoring

33.1 Ongoing monitoring is an intrinsic part of the CDD process. It must be performed on all matters, regardless of their individual risk rating, in order to detect unusual or suspicious transactions.

33.2 It is made up of two limbs:

33.2.1 scrutinising transactions throughout the course of the business relationship (including, where necessary, the source of funds) to ensure they are consistent with what you know about the client, their business and risk profile; and

33.2.2 undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD measures up-to-date.

33.3 Why is it necessary?

33.3.1 CDD and monitoring obligations are designed to make it more difficult for our firm to be used for money laundering or terrorist financing purposes.

33.3.2 As well as being a regulatory requirement, ongoing monitoring of client activity can help us to:

(a) identify unusual or suspicious behaviour warranting further investigation—if there appears to be no rational explanation for unusual or suspicious behaviour, the matter may involve money laundering or terrorist financing;

(b) know our clients—really knowing and understanding who our clients are can help to guard against fraud and the risk of committing offences under POCA 2002 and TA 2000 and it can also help us to provide a better service to those clients;

(c) assess risk—we have an obligation to keep our firm-wide risk assessment under review to ensure it remains up to date and relevant and we can use information obtained through our ongoing monitoring in that process;

(d) feel more confident that our firm is not being used for financial crime purposes; and

(e) assist law enforcement agencies—the more we know about our client and their activities, the more we can help with enquiries from the authorities.

33.4 How do we conduct ongoing monitoring?

33.4.1 AML Guidance for the Legal Sector says that a high degree of professionalism and scrutiny is expected from legal professionals; referring to fulfilling these obligations 'up to the hilt'.

33.4.2 The essential components of our system of monitoring are:

(a) aiming through our client and matter inception procedures to have as full as possible understanding of our client and the intended nature of the business relationship with them—in most cases this will be self-evident, but sometimes we may need to obtain additional information at the CDD stage (see section 28)

(b) ensuring we have up-to-date CDD information/documentation

33.4.3 Ongoing monitoring for standard and low risk clients/matters is usually carried out by the fee earner conducting the matter, as they are likely to have the best information and most current knowledge of the client and matter.

33.4.4 In practical terms, for a standard or low risk client and matter, it involves knowing as much as possible about the client and matter, remaining vigilant to anything unusual and ensuring CDD documentation remains up-to-date.

33.4.5 Don't forget that we have an obligation to look at CDD for existing clients from time to time on a risk-sensitive basis and including where you become aware that the circumstances of an existing client have changed in a way that is relevant to your assessment of risk for that client.

See section: 14.

33.5 What is enhanced ongoing monitoring and when is it required?

Enhanced ongoing monitoring is required for high-risk clients. It involves:

33.5.1 ensuring payments in a retainer are from an account in the client's name and are for an amount commensurate with the client's known wealth—ask further questions if they are not. Our Finance team is responsible for this

33.5.2 carrying out more frequent reviews of high-risk matters—we do this through *our file audit process*

33.5.3 closer involvement of the nominated officer in the matter, and/or

33.5.4 generally remaining aware of the high-risk nature of the matter and asking relevant questions if and when the need arises

33.5.5 remaining alert to public information relating to possible changes in the status of clients, particularly with regard to political exposure—eg new and existing clients who do not initially meet the definition of a PEP may become a PEP during the course of our business relationship with them

33.6 Discovering a discrepancy in CDD information

33.6.1 If, during the course of conducting ongoing monitoring, you discover any discrepancy between the CDD information collected and information held on relevant registers (eg Companies House register), you must make a report to the nominated officer. See section: 32

34 Receiving funds from the client or a third party

34.1 We do not provide banking facilities through our client account. Payments into, transfers to or withdrawals from our account must be in respect of instructions relating to a transaction or other service. We will not accept funds in any other circumstance from any source whatsoever.

34.2 When can I accept funds from my client?

34.2.1 You must not accept funds from or transfer funds to a client until the CDD process is complete.

34.3 When can I accept funds from a third party?

34.3.1 Payments from third parties where you cannot verify the source of the funds or where there does not appear to be a legitimate reason may be a warning sign of money laundering or terrorist financing.

34.3.2 You should satisfy yourself that the third party funds are coming from a legitimate source for legitimate reasons. As a first step you should consider:

(a) are there any obvious warning signs?
(b) what do you know about the client, the third party and their relationship?
(c) why is the third party giving money to the client?
(d) what is the proportion of funding being provided by the third party?
(e) how did the third party obtain the funds?

34.3.3 It may be appropriate to conduct CDD on the third party and/or ask for evidence to support any explanations provided by the client.

34.3.4 Supporting evidence might include:

(a) bank statements;

(b) filed business accounts;

(c) information confirming the sale of a house or shares;

(d) confirmation of inheritance or judicial award.

34.3.5 Where this is provided, you should check that the evidence is consistent with the client's explanation. Where there is any inconsistency you must consider whether you need to submit a SAR to the nominated officer.

34.3.6 If you are in any doubt please contact the nominated officer.

34.4 When can I accept cash?

34.4.1 Large amounts of cash can be a warning sign of money laundering or terrorist financing.

34.4.2 You can accept cash only in accordance with our Cash policy

35 Responding to investigations

35.1 The MLR 2017 require us to establish and maintain systems to enable us to respond rapidly and fully to enquiries from investigators and other enforcement officers, including:

35.1.1 whether you maintain, or have maintained during the previous five years, a business relationship with any person, and

35.1.2 the nature of that relationship

35.2 Our CDD record-keeping arrangements (see section 17) together with the information we store on our Practice Management system enable us to fulfil this requirement.

35.3 You must refer any requests from investigatory authorities immediately to the nominated officer.

36 Screening relevant employees

36.1 The MLR 2017 require us to carry out screening of relevant employees where it is appropriate.

36.2 We may carry out screening:

36.2.1 before an employee is appointed; and

36.2.2 during the course of the appointment.

36.3 We will always carry out screening where we apply for SRA approval of any new beneficial owner, officer or manager. This will involve conducting a basic DBS check on that person.

37 Training and awareness

37.1 The MLR 2017 require us to provide training on money laundering and terrorist financing.

37.2 All relevant employees and agents will be:

37.2.1 made aware of the law relating to money laundering, terrorist financing and data protection

37.2.2 trained regularly (at least every year) on how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing

37.3 Training is provided online and/or through seminars

37.4 Completion of training is compulsory.

37.5 The nominated officer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our AML/CTF policy and procedures, please contact the nominated officer.

38 Monitoring and reviewing this policy

38.1 How will compliance with this policy be monitored?

Compliance will be continually monitored through any or all of the following methods:

38.1.1 file audits

38.1.2 review of records maintained by the nominated officer

38.1.3 reports or feedback from staff

38.1.4 any other method

38.2 Policy review

38.2.1 We will review this policy at least annually as part of our overall risk management process. We will also review this policy if:

(a) there are any major changes in the law or practice

(b) we identify or are alerted to a weakness in the policy

(c) there are changes in the nature of our business, our clients or other changes which impact on this policy

39 Further information

39.1 You can get further advice and guidance from the nominated officer.

APPENDIX 1
INTERNAL
SUSPICIOUS ACTIVITY
REPORT FORM

SAR Reference Number:	[insert number]

A record of this Suspicious Activity Report (SAR) will be kept by the nominated officer for at least five years.

You must use this form in every case where you know or suspect that another person is engaged in money laundering or terrorist financing or where you have knowledge or suspicion of:

—bribery or corruption

—property or mortgage fraud

—slavery or human trafficking

—organised crime group involvement, or

—tax evasion facilitation

If you are unsure as to whether you have such a suspicion, please do not use this form but instead seek guidance from the nominated officer.

1 General (complete all sections)

Date SAR submitted to the nominated officer	[insert date]
Your name	[insert name]
Branch/office	[insert details]
SAR type (money laundering/terrorist financing/property or mortgage fraud/bribery or corruption/slavery or human trafficking/organised crime/other—please state)	[insert SAR type]
Customer/client name	[insert name]
Customer/client/matter reference number	[insert number]
Department dealing with the matter	[insert details]
Do you require consent/a defence to continue with the matter? If yes, set out all the steps that you need to take to complete the matter where prompted in section 6 below	Yes/No

Does this SAR relate to a previous SAR? If yes, please provide details	Yes/No [insert details]

2 Details of the main subject of this SAR (complete as much as you are able)

Does this SAR relate to a suspect or a victim?	[insert suspect or victim]
Is the subject of this SAR: —an individual?—If yes, please go to 3 —a legal entity?—If yes, please go to 4	[insert individual or entity]
Are there any individuals or entities who are associated with the main subject? If yes, complete details in 5	Yes/No

3 Individual

Full name	[insert name]
Date of Birth (dd/mm/yyyy)	[insert date]
Gender	[insert details]
Occupation	[insert details]
Full address	[insert details]
Address type (home/business/other)	[insert home/business/other]
Is this address current?	Yes/No/Unsure
Any other identification details (eg passport, driving license or NI number)	[insert details]

4 Legal entity

Full name	[insert name]
Company number	[insert number]
VAT number	[insert number]
Country of registration	[insert details]
Full address	[insert details]
Is this address current	Yes/No/Unsure

Type of business	[insert details]
Any other identification details	[insert details]

5 Associated subjects (complete if appropriate)

Details of any associated subjects (ie people or entities you believe are linked to the main subject above and are involved in the criminal activity), including identifying information as above and details of the nature of the association with the main subject	[insert details]

6 Details of knowledge/suspicion

Does your knowledge or suspicion relate to a specific offence? If yes, please indicate: drugs/fraud/terrorism/bribery/slavery/organised crime/other (please state)	Yes/No [insert details]
Have you discussed your knowledge or suspicions with any person other than the nominated officer? If yes, please give details (who/why/when, etc)	Yes/No [insert details]
What is the nature of the property you suspect is criminal property, if applicable? Money/other property—please state	[insert money/other property]
Do you know the whereabouts of the property, if applicable? If yes, please provide details (eg in the case of money, the account details of where it is held)	Yes/No [insert details]
Please set out your reasons for making this SAR in as much detail as possible Who/what/where/when/how/why, etc	[insert details]
Please explain the act(s) involving suspected criminal property that you are seeking consent/defence for (if applicable)	[insert details]
Signed and dated (discloser)	[signature and date (dd/mm/yyyy)]

Signed and dated (nominated officer)	[signature and date (dd/mm/yyyy)]

APPENDIX 2
CLIENT DUE DILIGENCE MATRIX

1 Introduction

Evidence of identity can be obtained in a number of forms and come from a number of sources. Whatever evidence you rely on, it must cause you to be reasonably satisfied as to someone's identity.

The documentation you require from clients will depend on the nature of the client and your assessment of the risk they present to your business. This may involve accepting a range of documents.

The Money Laundering Regulations 2017 (MLR 2017) set out a summary of the risk factors which you should take into account when conducting client due diligence, together with AML Guidance for the Legal Sector, based on the Law Society 2013 AML practice note, which was published by the Legal Sector Affinity Group, approved by HM Treasury in March 2018. The Group comprises the AML supervisors for the legal sector. The Guidance applies across the legal services sector and replaces previous guidance.

This is especially true in relation to politically exposed persons (PEPs) and when it comes to contraventions of the MLR 2017.

You must consider the CDD measures to put in place, which may differ from case to case. You:

1.1 must take into account relevant information made available to you by your supervisory authority; and

1.2 you may take into account any guidance which has been issued by the FCA, or any other supervisory authority or appropriate body and approved by HM Treasury

In deciding whether there has been a contravention of the requirements of the MLR 2017 a court or regulator must consider whether you have followed such guidance.

You should use this document as a guide to help you decide on the level of client due diligence (CDD) to apply and what documentary evidence to request/accept from a client or potential client.

2 Key

CDD	Client due diligence
EDD	Enhanced due diligence
SDD	Simplified due diligence
RDD	Regular due diligence

3 Individuals

This section contains CDD measures for private individuals which must be followed in every case:

Client type	Requirement	Actions
UK individual	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Electronic Verification and if EDD either Facial Recognition app or obtain one document from list **A** and one document from list **B** **A** —current signed passport —current photocard driving licence —birth certificate —marriage certificate **B** —current photocard driving licence —council tax or utility bill —bank, building society, mortgage or HMRC tax statement —house or motor insurance certificate —record of home visit
Well-known individual (eg a celebrity)	AML Guidance for the Legal Sector appears to suggest that SDD may be appropriate.	Record a file note of your satisfaction about identity, including an address.

Overseas individual	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures, eg where you do not meet the client—see Individual who you do not meet faceto-face below. If documents are in a foreign language you must take appropriate steps to be reasonably satisfied that the	Electronic Verification and either Facial Recognition app or obtain one document from list **A** and one document from list **B** **A** —current signed passport —current national identity card

Client type	Requirement	Actions
	documents in fact provide evidence of the individual's identity. If in doubt, ask for them to be translated.	—birth certificate **B** —council tax or utility bill —bank, building society, mortgage or HMRC tax statement —house or motor insurance certificate —official, reputable overseas directory —confirmation of address from a regulated person in the relevant jurisdiction

Overseas individual based in a high-risk third country, as identified by the European Commission	You must apply EDD.	Electronic Verification and either Facial Recognition app or obtain one document from list **A** and one document from list **B** **A** —current signed passport —current national identity card —birth certificate **B** —council tax or utility bill —bank, building society, mortgage or HMRC tax statement —house or motor insurance certificate —official, reputable overseas directory

Client type	Requirement	Actions
		—confirmation of address from a regulated person in the relevant jurisdiction **and** —document your examination of the background and purpose of the matter —ensure you increase the degree and nature of ongoing monitoring in relation to the client's matters Depending on the level of risk you have identified, you may also wish to: —seek additional independent, reliable sources to verify information provided by the client —take additional measures to understand better the background, ownership and financial situation of the client and other parties to the transaction —take further steps to be satisfied that the matter is consistent with the purpose and intended nature of the business relationship

Agent or representative of an individual	RDD applies unless you have identified circumstances in your risk assessment that trigger the need for EDD measures.	Obtain: —verification that the representative is authorised to act on the client's behalf —evidence of identify the representative, and —verification of the identity of the representative on the basis of documents or information obtained from a reliable source which is independent of both the person and the client

Professional, instructing you in their capacity as a professional (not as a private individual)	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate)—a professional individual is not one of those factors.	Obtain: —verification that the representative is authorised to act on the client's behalf —evidence of identify the representative, and —verification of the identity of the representative on the basis of documents or information obtained from a reliable source which is independent of both the person and the client

Politically exposed person (PEP)	You must apply EDD	Obtain: —the required documents as for individual above (whether in the UK or overseas), and —the approval of the Nominated Officer to accept the instructions Take adequate steps to establish the source of wealth and source of funds which are involved in the business relationship. Consider whether there are signs of corruption or evidence that government or state funds are being used inappropriately, **and** Conduct enhanced ongoing monitoring—keep a closer eye on the matter

Individual who you do not meet face-to-face	You must consider applying EDD.	Obtain the required documents as for an individual above (whether in the UK or overseas), **and either:** —require that the documents provided are certified by a lawyer, bank manager, accountant or GP whose identity you can check by reference to a professional directory, or —electronically verify the client's identity **and** —ensure the first payment in a retainer is from an account in the client's name with a UK or EU regulated credit institution or an assessed low risk jurisdiction

Individual who is unable to produce standard documentation	Entirely dependent on your risk assessment for the specific client and their circumstances.	Consider whether the inability to provide you with standard verification is consistent with the client's profile and circumstances or whether it might make you suspicious that money laundering or terrorist financing is occurring. Obtain a letter from an appropriate person who knows the individual and can verify their identity, eg: —care home manager —hostel manager/staff —Home Office —priest, GP or local councillor —social worker —guardian appointed by the court

4 Partnerships, LLPs and companies

This section contains required guidelines CDD measures for partnerships, limited liability partnerships (LLPs) and companies:

Client type	Requirement	Actions
UK credit or financial institution	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate) and a credit institution or a financial institution which is (i) subject to the requirements in national legislation implementing 4MLD as an obliged entity, and (ii) supervised for compliance with those requirements, is one of those factors.	Speak to AMLRO/ALMCO
Credit or financial institution in the EEA	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into	Speak to AMLRO/ALMCO

	account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate) and a client established, registered or operating in a third country which has effective systems to counter money laundering and terrorist financing is one of those factors. Note requirement to apply enhanced due diligence (EDD) where the client is based in a high-risk third country, as identified by the European Commission. For details on which countries are currently considered high-risk, see Table of high-risk countries.	

Credit or financial institution outside the EEA where equivalent AML provisions apply	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate) and a client which is established, registered or operating in a third country which has effective systems to counter money laundering and terrorist financing is one of those factors. Note requirement to apply EDD where the client is based in a high-risk third country, as identified by the European Commission. For details on which countries are currently considered high-risk, see Table of high-risk countries.	Treat as credit or financial institution in the EEA.

Credit or financial institution outside the EEA where there are *no* equivalent AML provisions	EDD may apply. The MLR 2017 set out factors to take into account when assessing whether there is a high risk of money laundering and terrorist financing (ie situations where EDD may be appropriate) and a client established, registered or operating in a country identified as not having effective AML/CTF systems is one of those factors. Note also the requirement to apply EDD where the client is based in a high-risk third country, as identified by the European Commission. For details on which countries are currently considered high-risk, see Table of high-risk countries.	As above **and** —document your examination of the background and purpose of the matter —ensure you increase the degree and nature of ongoing monitoring in relation to the client's matters Depending on the level of risk you have identified, you may also wish to: —seek additional independent, reliable sources to verify information provided by the client —take additional measures to understand better the background, ownership and financial situation of the client and other parties to the transaction —take further steps to be satisfied that the matter is consistent with the purpose and intended nature of the business relationship

UK partnership	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Obtain: —full name —business address —names of all partners/principals who exercise ultimate control over the management of the partnership

Client type	Requirement	Actions
		—names of individuals who own or control over 25% of its capital, profits, or voting rights Take reasonable steps to verify the identity of the partners. For smaller partnerships, treat as a collection of individuals (see section 3 above). For larger partnerships, consider makeup, eg is it made up of professionals? (See UK partnership made up of regulated individuals (eg solicitors, accountants, etc) below.) If not, treat as private unlisted company. For all sizes and natures of partnership, have sight of the partnership deed or equivalent.

UK partnership made up of regulated individuals (eg solicitors, accountants, etc)	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate)—a professional individual is not one of those factors.	[*Insert required actions—see Drafting Note*]
Well-known, reputable partnerships	SDD **may** apply, depending on your risk assessment.	Record: —name

Client type	Requirement	Actions
		—registered address, if any —trading address —nature of business —the names of all individual beneficial owners owning/controlling more than 25% of the capital, profit or voting rights or who otherwise exercise control Take reasonable steps to verify the identity of beneficial owners.

UK private unlisted company (ltd) and UK LLP	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Obtain and verify: —the name of the body corporate —its company number or other registration number —the address of its registered office, and if different, its principal place of business Take reasonable measures to determine and verify: —the law to which it is subject (whether set out in its articles of association or other governing documents) —the full names of the board of directors or equivalent and the senior persons responsible for the operations of the body corporate —identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner so that you are

Client type	Requirement	Actions
		satisfied you know who the beneficial owner is —if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement Verification sources for identifying UK private unlisted companies include: —certificate of incorporation —details from the relevant company registry, confirming details of the company and of the director(s) and their address(es) —filed audited accounts —information from a reputable electronic verification service provider

Subsidiary of existing private unlisted company for whom CDD has been conducted	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate)—a subsidiary of existing private unlisted company for whom CDD	This will depend on: —your risk assessment —the information you already hold —whether the existing client has been identified to the standards of the MLR 2017 If the client is a body corporate, obtain and verify: —its name —the company number or other registration number, and

Client type	Requirement	Actions
	has been conducted is not one of those factors.	—the address of the registered office and, if different, principal place of business Consider the identity of beneficial owners.

Company on a listed regulated market	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment.	Obtain and verify: —its name —the company number or other registration number, and —the address of the registered office and, if different, principal place of business Obtain confirmation of the company's listing, eg: —a copy of the dated page of the website of the relevant stock exchange showing the listing —a photocopy of the listing in a reputable daily newspaper, or —information from a reputable electronic verification service provider or online registry There is no requirement to take any steps in relation to the beneficial owner.
Majority-owned and consolidated subsidiaries of companies listed on regulated markets in the UK, EEA or non-EEA market that is subject to specified disclosure obligations	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment.	Obtain evidence of the parent/subsidiary relationship, eg —the subsidiary's last filed annual return

Client type	Requirement	Actions
		—a note in the parent's or subsidiary's last audited accounts —information from a reputable electronic verification service provider or online registry —information from the parent company's published reports, eg from its website
Other publicly listed or quoted companies	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. Note requirement to apply EDD where the client is based in a high-risk third country, as identified by the European Commission. For details on which countries are currently considered high-risk, see [*Table of high-risk countries*].	Obtain and verify: —its name —the company number or other registration number, and —the address of the registered office and, if different, principal place of business You may consider that the listing conditions that apply in the relevant jurisdiction and the level of transparency and accountability to which the company is subject in determining the level of checks and the extent to which you treat the client as a private company or a public company. In principle the obligation to verify beneficial owners applies here.

Overseas private unlisted companies	RDD applies unless you have identified circumstances in your CDD risk assessment that triggers the need for EDD measures. Note requirement to apply EDD where the client is	Obtain documentation as for UK private unlisted company above but be aware of any increased risks presented as a result of the country in which the client is incorporated. These are likely to be lower where the client is incorporated or

Client type	Requirement	Actions
	based in a high-risk third country, as identified by the European Commission. For details on which countries are currently considered high-risk, see [*Table of high-risk countries*].	operating in an EEA state or a country which is a member of FATF. Where you are not obtaining original documentation, consider on a risk-sensitive basis, having the documents certified by a person in the regulated sector or another professional whose identity can be checked by reference to a professional directory.
Companies with capital in the form of bearer shares	EDD **may** apply, depending on your risk assessment.	—obtain documentation as for UK private unlisted company above **and** —establish the identities of the holders and material beneficial owners of the shares **and** —obtain an undertaking that you will be notified whenever there is a change of holder and/or beneficial owner

Well-known 'household name' company or partnership (ie the entity is well-known, reputable, has a long history in its industry and there is substantial public information about them)	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate)—a 'household name' is not one of those factors.	Speak to AMLRO/ALMCO

5 Other arrangements or bodies

This section contains guidelines CDD measures for other arrangements or bodies:

Client type	Requirement	Actions
UK trust	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Obtain the following information: —name of the settlor —full name of the trust —nature, purpose and objects of the trust (eg, discretionary, testamentary, bare) —country of establishment —names of all trustees —names of any beneficiaries (or, where relevant a description of the class of beneficiaries) —name and address of any protector or controller Verify the identity of the trust on the basis of documents or information obtained from a reliable source which is independent of the client, eg requiring sight of relevant extracts from the trust deed, or reference to an appropriate register in the country of establishment. Take reasonable measures to understand the

		ownership and control structure of the client. Take reasonable measures to understand the ownership and control structure of the client. Verify the identity of the beneficial owners (in most cases this will be the trustees, beneficiaries and settlor). Where there are a large number of beneficial owners, on a risk based approach, determine who/how many to apply this requirement to.

Client type	Requirement	Actions
Non–UK trust	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Obtain the following information: —settlor —full name of the trust —nature, purpose and objects of the trust (eg, discretionary, testamentary, bare) —country of establishment —names of all trustees —names of any beneficial owners —name and address of any protector or controller Verify the identity of the trust on the basis of documents or information obtained from a reliable source which is independent of the client, eg requiring sight of relevant extracts from the trust deed, or reference to an appropriate register in the country of establishment. Take reasonable measures to understand the ownership and control structure of the client. Verify the identity of the beneficial owners. Where there are a large number

		of beneficial owners, on a risk based approach, determine who/how many to apply this requirement to.

Client type	Requirement	Actions
Foundation	CDD level is dependent on the nature and purpose of the foundation and the legal form it takes.	Speak to AMLRO/ALMCO
Registered charities, church bodies and places of worship	CDD level is dependent on the nature and purpose of the body and the legal form it takes.	Speak to AMLRO/ALMCO
Unregistered charities	CDD level is dependent on the nature and purpose of the charity and the legal form it takes.	Consider the business structure and conduct appropriate CDD as set out for companies, trusts, etc above.
Deceased persons' estates	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	The court documents granting probate or letters of administration can be sufficient as evidence of the identity of those personal representatives. You should also —establish the identity of executors or administrators using the procedures for natural persons or companies —where you act for more than one executor or administrator, verify the identity of at least two of them —consider getting a copy of the death certificate
Schools or colleges	CDD level dependent on the legal form it takes.	As appropriate, see CDD requirements for charities, private

		companies, etc.
Clubs, associations and societies	RDD applies unless you have identified circumstances in your CDD risk assessment that trigger	Obtain and record: —full name

Client type	Requirement	Actions
	the need for EDD measures or the ability to apply SDD.	—legal status —purpose —registered address —names of all office holders To verify the existence of the club etc, obtain: —articles of association or constitution —statement from a bank, building society or credit union —recent audited accounts —financial statements presented to the annual general meeting, and/or —listing in a telephone directory**]** Verify the identities of the officers who have authority to give the firm instructions concerning the use or transfer of

		funds or assets. Where the risk is higher, verify the identities of additional officers, and/or institute additional ongoing monitoring arrangements.
Employee pension funds	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment. The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering	Obtain evidence that the product is a scheme that qualifies for SDD, eg: —copy of a page showing the name of the scheme from the most recent definitive deed, or —consolidating deed for the scheme, plus any amending deed subsequent to that date, from which you can

	and terrorist	

Client type	Requirement	Actions
	financing (ie situations where SDD may be appropriate)—a pension, superannuation or similar scheme is one of these factors where: —the scheme provides retirement benefits to employees —contributions to the scheme are made by way of deductions from wages, and —the scheme rules do not permit the assignment of a member's interest under the scheme	assess how contributions are made and members' interest assignment rights For pension schemes that do not tick all the boxes, see below.

Other pension funds	SDD cannot apply under MLR 2017, reg 36(3)(b)(iii) so RDD applies unless you have identified circumstances in your CDD risk assessment that trigger the need for EDD measures.	Where a pension scheme does not meet the criteria above and therefore you are not able to apply SDD measures, you must apply CDD as appropriate to the business structure. You could also consider taking the following measures, depending on your risk assessment: —seeking confirmation of registration with HMRC or the Pensions Regulator —verifying the identity of the principal employer —verifying the source of funding
UK or overseas governments, supranational organisations, government departments, state-owned companies or local authorities, including:	SDD **may** apply, depending on your risk assessment. There is no automatic entitlement to apply SDD in any situation, each must be subject to risk assessment.	Obtain: —full name —nature and status (eg, overseas government, treaty organisation, etc) —address

Client type	Requirement	Actions

—state supported schools, colleges and universities, and —NHS trusts	The MLR 2017 set out factors to take into account when assessing whether there is a low risk of money laundering and terrorist financing (ie situations where SDD may be appropriate)—a public administration or publicly owned enterprise is one of those factors.	—name of the home state authority, and —names of directors (or equivalent) —name of the individual instructing you and confirmation of their authority to do so —extract from official government website Take appropriate steps to understand the ownership of the client and the nature of its relationship with its home state authority. Where appropriate, verify the identities of the directors (or equivalent) who have authority to give instructions in relation to funds or assets.

Public authorities, etc based in a high-risk third country, as identified by the European Commission	You must apply EDD.	As above, **and** —document your examination of the background and purpose of the matter —ensure you increase the degree and nature of ongoing monitoring in relation to the client's matters Depending on the level of risk you have identified, you may also wish to: —seek additional independent, reliable sources to verify information provided by the client —take additional measures to understand better the background, ownership and financial situation of the
Client type	Requirement	Actions
		client and other parties to the transaction —take further steps to be satisfied that the matter is consistent with the purpose and intended nature of the business relationship

APPENDIX 3
SOURCE OF FUNDS STATEMENT

Please complete and return this form as soon as possible.

Customer(s)/Client(s) full name(s) or entity name(s) for corporate borrower(s):	[*insert name*]
Please provide details of how the initial funds have been generated by you: *Please include full details (amounts, dates, employer details, transaction details, third party details etc).* Please note that we may ask you to provide three months' bank statements or other documents to support the details you provide**[** and if you are using a gift from a parent or other family member, we will notify your lender so you must ensure it is agreed by them before instructing us**]**.	
Main geographic region or country from which the funds were generated:	[*insert details*]
For company structures only, reason for the financial structure:	[*insert details*]
Signature:	
Print name:	[*insert name*]
Date:	[*insert date*]