Addendum to the Legal Sector Affinity Group Anti-Money Laundering Guidance for the Legal Sector, Part 2a Specific Guidance for Barristers and Advocates, 2021

This document is an addendum to the 2021 edition of the Legal Sector Affinity Group, Part 2a Specific Guidance for Barristers and Advocates. It is provided as an update prepared by the Bar Council of England and Wales, the Bar Council of Northern Ireland, the Faculty of Advocates in Scotland and the Bar Standards Board and is issued by the Legal Sector Affinity Group. The update illustrates how our attitude towards regulation is developing over time. The changes below are currently pending approval by HM Treasury and, if accepted, will be integrated into the text of the main guidance. Until approval by HMT, this addendum is supplementary to the main Part 2a guidance and does not supersede it. It is not for your supervisor to provide specific legal advice and/or confirmation on the application of the money laundering regulations (MLRs) or other regulation or legislation. You must satisfy yourself on your legal/regulatory obligations under the MLRs and that you have complied with them. While care has been taken to ensure that this addendum is accurate, up to date and useful, members of the LSAG will not accept any legal liability in relation to it.

The authors have considered the changes made by the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022. We have also amended Annex 1 of our guidance to reflect changes made to the Part 1 LSAG guidance relating to customer due diligence.

In addition, the authors have produced updated Frequently Asked Questions (FAQs), including changes to the FAQs on customer due diligence and real property and additional questions relating to proliferation financing and enfranchisement, and two additional typologies on real property. Both the FAQs and the typologies can be found in a separate addendum.

Our proposed amendments to the approach set out in the Part 2a guidance are as follows. While this does not supersede the HM Treasury-approved LSAG guidance, we suggest that the following is an appropriate interpretation.

In the following:

- text which is struck through is a proposed deletion.
- text in bold is a proposed addition.

EXECUTIVE SUMMARY

Introduction

[ADDITIONAL PARAGRAPH] **.5 Proliferation financing is the act of providing certain funds or financial services for use in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in**

connection with the possession or use of, chemical, biological, radiological or nuclear weapons (CBRN) including the provision of certain funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology.

Essential Matters

6. It is the duty of every barrister and advocate to understand the principles of money laundering, ~~and~~ terrorist financing **and proliferation financing (a full definition and further explanation of proliferation financing is given at 5.3.1 of the Part 1 Guidance)** and how to recognise them. The essential principles are set out in this document.

7. Every barrister and advocate owes an obligation not to become involved in money laundering~~, or~~ terrorist financing **or proliferation financing**. These concepts are broadly defined. There is authority from the Court of Appeal of England and Wales that the "*ordinary conduct of litigation*" does not fall within the concept of becoming concerned in a money laundering arrangement under s.328 of POCA, which will mean that most of the things that you do as a barrister or advocate will not trigger anti-money laundering or counter-terrorist financing obligations. However, you should be alert to circumstances that may take litigation out of the "*ordinary*" and note that the "*ordinary conduct of litigation*" exception does not apply to activities performed outside a litigation or arbitration context.

9. While the risk of a barrister or advocate becoming involved in conduct that involves money laundering~~, or~~ terrorist financing **or proliferation financing** is relatively low (in particular because barristers and advocates are not permitted to handle client money or manage their affairs) some risk remains. You must know how to address those risks and how and when to take the correct and necessary action when such risks arise.

10. If your practice is in England and Wales you must act in compliance with the anti-money laundering, ~~and~~ counter-terrorist financing **and proliferation financing** requirements of the BSB and the BSB Handbook. If your practice is in Scotland you must comply with the Faculty's Guide to Professional Conduct and if your practice is in Northern Ireland you must observe the requirements of the Bar of Northern Ireland's Code of Conduct.

Risk Assessment

23. You must carry out a risk assessment **(risk assessments for money laundering, terrorist financing and proliferation financing)** in relation to work within the scope of the Regulations. This assessment should take into account risk factors including those relating to the client, the countries or areas in which you practise, the nature of the services you offer, the type of transactions you advise on and the source of your

Commented [AD1]: Para 23 has been amended but has lost tracking

instructions. You must keep an up-to-date record of the steps you have taken in this regard.

Enhanced Due Diligence

27. There may be circumstances where the risk of money laundering, ~~or~~ terrorist financing **or proliferation financing** is such that you may need or will be obliged to apply an enhanced level of CDD, for example where the lay client is based in or operating from a country that is known to present such a risk or is a Politically Exposed Person ["PEP"]. In those circumstances you will need to apply greater due diligence to mitigate the increased level of risk.

Risks and Indicators

30. Potential indicators of money laundering, ~~or~~ terrorist financing **or proliferation financing** activity will come in a variety of forms but may include: the lay client being based in a high- risk country or region; the nature of the business operated by the lay client; the source of funds involved in the transaction or the personal circumstances of the lay client or someone involved in your instructions.

Reliance

32. Where you act upon the instructions of a professional client, such as a solicitor, it may be possible, with **appropriate arrangements in place** ~~their consent,~~ to rely on the CDD that they have carried out. However, if you do, you remain legally responsible for the regulatory compliance of the checks undertaken and therefore for any failings in them. You must therefore ensure that you have complied with Regulation 39**, in particular, you are in a position to meet the requirements in Regulations 39(2)** ~~and obtained the necessary "information" to satisfy, on a risk-based approach, the CDD obligations upon you.~~

Other Obligations Under the Regulations

34. Where you are undertaking work that falls within the scope of the Regulations you may commit a criminal offence if:

(i) you suspect that money laundering **(including proliferation financing)** is taking place and you fail to make the required disclosure to the authorities (s.330), or

(ii) you make an unauthorised disclosure of your suspicion of money laundering or of your knowledge of a money laundering **(including**

proliferation financing) investigation to another person (aka "*tipping-off*") (s.333A).

Making a Disclosure

36. Where you are required to make a disclosure of suspected money laundering, **terrorism or proliferation financing** or money laundering, **terrorism or proliferation financing** this must be done by way of making a Suspicious Activity Report ["SAR"] to the NCA. Such reports should be made electronically via the NCA's website.

DETAILED GUIDANCE

THE MONEY LAUNDERING, TERRORIST FINANCING AND TRANSFER OF FUNDS (INFORMATION ON THE PAYER) REGULATIONS 2017

Independent legal professionals

PRA Risk Assessment

[ADDITIONAL PARAGRAPH] **26. You must carry out a PRA risk assessment in relation to work within the scope of the Regulations see [23] in the Executive Summary above.**

That risk assessment should be specific to your practice, recorded in writing and reviewed in order to keep it up to date. You should keep a written record of the dates that it is reviewed and the actions taken.

To assess the level of risk you should consider all the relevant AML/CTF/CPF risk factors as they are apparent to you in your practice and the instructions that you receive. Those factors must include the mandatory factors under reg. 18(2) and 18A(2).

Policies, Controls and Procedures

26. **Having completed a PRA, w**here your practice brings you within the scope of the Regulations you must establish and maintain written policies, controls and procedures to mitigate and manage effectively the risks of money laundering, ~~and~~ terrorist financing **and proliferation financing** identified in your reg. 18 **and reg. 18(A)** risk assessments (reg. 19(1) **and 19A(1)**).

Proportionality: Risk Profile

27. The policies, controls and procedures established by you must be proportionate to the size and nature of your practice as it falls within the scope of the Regulations (reg. 19(2)(a) and 19A(2)(a)). In determining what is appropriate or proportionate with regard to

the size and nature of your practice **in respect of money laundering and terrorist financing,** all advocates and barristers may take into account this Guidance (reg. 19(5)). Barristers in England and Wales may also consider the BSB's AML/CTF Risk Assessment for the profession **in respect of money laundering and terrorist financing** (reg. 19(5)). The BSB's current assessment places the overall risk of money laundering for barristers as "low".[1] However, that does not mean that the risk in your practice or any matter in which you are instructed is at the same level. You must determine what is appropriate or proportionate in relation to the risk of your practice and avail of any risk assessments undertaken by the relevant supervisor in your jurisdiction.

Mandatory requirements

28. The policies, controls and procedures established by you must include:

(i) risk management practices;

(ii) internal controls;

(iii) **(in relation to money laundering and terrorist financing)** CDD, *i.e.* the means by which you check and verify your client's identity

(see [57] *et seq* below). **In relation to proliferation financing, it is prudent (not mandated) to establish such a policy, control and procedure to ensure the CDD obligations will be met in practice**;

(iv) **(in relation to money laundering and terrorist financing)** ~~reporting~~ **reliance** and record keeping. **In relation to proliferation financing, it is prudent (not mandated) to establish such a policy, control and procedure will be met in practice**; and

(v) the monitoring and management of compliance with, and the internal communication of, such policies and procedures (reg. 19(3) **and 19A(3)**).

29. The policies, controls and procedures must also:

(i) provide for the identification and scrutiny of any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose. They must also provide for the identification and scrutiny of any other activity that you regard as particularly likely by its nature to be related to money laundering,~~ or~~ terrorist financing **and proliferation financing** (reg. 19(4)(a) **and 19A(4)(a)**);

[1] https://www.barstandardsboard.org.uk/for-barristers/compliance-with-your-obligations/anti-money- laundering-counter-terrorist-financing.html

(ii) specify the taking of additional measures, where appropriate, to prevent the use for money laundering, ~~or~~ terrorist financing **and proliferation financing** of products and transactions which might favour anonymity (reg. 19(4)(b) and **19A(4)(b)**);

(iii) ensure that when you adopt new products, business practices (including new delivery mechanisms) or technology, you take appropriate measures to assess and if necessary mitigate any money laundering, ~~or~~ terrorist financing **and proliferation financing** risks the new product, practice, or technology may cause (reg. 19(4)(c) **and 19A(4)(c)**); and

(iv) ensure that anyone employed by you or your chambers or entity who, as a result of information received by them as a result of or in the course of your practice, knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is engaged in money laundering or terrorist financing is required to comply with Part 3 of TA or with Part 7 of POCA (reg. 19(4)(d)).

Determining Appropriateness

31. In determining what risk-management systems and procedures are "appropriate" under the Regulations you must, pursuant to reg. 35(2), take account of:

(i) the risk assessment you carried out in respect of your practice under reg. 18 **and 18A**;

(ii) the level of risk of money laundering and terrorist financing inherent in your practice **whilst it would be prudent (not mandatory) to take account of the level of risk of proliferation financing inherent in your practice**;

BSB entities

32. In addition to the above and in England and Wales, BSB entities should consider whether the nature of their organisation requires them to comply with the obligation to communicate the policies, controls and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom (reg. 19(6) **and 19A(5)**).

Additional Internal Controls

Application

39. A "relevant employee or agent" is defined by Regulation 21(2)(b) as an employee or agent whose work is:

(i) relevant to your compliance with any requirement under the Regulations, or

(ii) otherwise capable of contributing to the

(a) identification or mitigation of the risks of money laundering, ~~and~~ terrorist financing **and proliferation financing** within your practice, or

(b) prevention or detection of money laundering, ~~and~~ terrorist financing **and proliferation financing** in relation to your practice.

41. Where the additional "internal controls" requirements of reg. 21 apply and where "appropriate with regard to the size and nature" of your practice, you must also establish an independent audit function with the responsibility—

(i) to examine and evaluate the adequacy and effectiveness of your AML/CTF**/CPF** policies, controls and procedures;

(ii) to make recommendations in relation to those policies, controls and procedures, and

(iii) to monitor your compliance with those recommendations (reg. 21(1)(c)).

Determining Appropriateness

(iv) In determining what is "appropriate with regard to the size and nature" of your practice: you must take into account your risk assessment under reg. 18(1) **and 18A(1)**; and

(v) you may take into account any relevant guidance which was at the time issued by the FCA, supervisory authority or appropriate body and approved by the Treasury **(reg 21(10)**, e.g. this Guidance. Pursuant to reg. 19(1), practitioners in England and Wales may also take into account the current BSB AML/CTF Risk Assessment **in relation to money laundering and terrorist financing**, see [27]above.

Duty of the Nominated Officer in BSB entities upon receipt of a disclosure

43. Where a disclosure is made to the nominated officer of a BSB entity, that officer must consider it in the light of any relevant information that is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering, or terrorist financing **or proliferation financing**.

Awareness and Training: Relevant Employees and Agents

48. Where you are subject to the Regulations you must take "appropriate" measures to ensure that relevant employees and agents are made aware of the law relating to money laundering, terrorist financing**, proliferation financing** and data protection and are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering, ~~or~~ terrorist financing **and proliferation financing** (reg. 24(1)). In Scotland this responsibility falls on Faculty Services Limited and not individual advocates unless they directly employ their own staff.

Determining Appropriateness

49. In determining what measures are "appropriate" you must take account of the size and nature of your practice and the attendant nature and extent of the risk of money laundering, ~~and~~ terrorist financing **and proliferation financing** (reg. 24(3)). You may also take into account any relevant guidance which was at the time issued by the FCA, supervisory authority or appropriate body and approved by the Treasury, e.g. this Guidance (reg. 24(3)(b)). Pursuant to reg. 19(1), practitioners in England and Wales may also take into account the current BSB AML/CTF Risk Assessment **in relation to money laundering and terrorist financing**, see [27] above.

50. A "relevant employee or agent" is an employee or agent whose work is defined by reg. 24(2) as:

(i) relevant to your compliance with any requirement under the Regulations, or

(ii) otherwise capable of contributing to the:

(a) identification or mitigation of the risks of money laundering, ~~and~~ terrorist financing **and proliferation financing** within your practice, or

(b) prevention or detection of money laundering, ~~and~~ terrorist financing **and proliferation financing** in relation to your practice (reg. 24(2)(a) &(b)). Chiefly this will mean your clerks.

51. Clerks and any other staff must regularly be given training to recognise and report suspected money laundering, ~~or~~ terrorist financing, **proliferation financing** and breaches of data protection law. The training provided must be of sufficient depth and quality to create a risk-aware culture and must be regularly reviewed.

52. Self-employed barristers practising from a set of chambers may opt to have chambers organise and provide the required training. However, the requirement for such awareness to be in place and training to be undertaken remains the responsibility of each individual barrister who makes use of the employee or agent's services whilst acting within the scope of the Regulations: it is a personal liability. Equally, should suspected money laundering, ~~or~~ terrorist financing **and proliferation financing** be reported to you by an employee or agent, you must personally assess and determine what to do about the information provided to you. The responsibility to ensure that the Regulations have been complied with and that the required CDD **(where applicable)** has been properly conducted falls upon each individual practitioner.

Risk Assessment

53. Where you are instructed in a matter that brings you within the scope of the Regulations you must:

(i) take appropriate steps to identify and assess the risks of money laundering, ~~and~~ terrorist financing **and proliferation financing** (regs. 18 **and 18A**);.

(ii) ~~In deciding what steps are "appropriate" you must T~~take into account the size and nature of your practice **in deciding what steps are "appropriate"** (regs. 18(3) **and 18A(3)**); **and**

(iii) **(take into account 5.3.1, 5.4.1. and 18.10 of the Part 1 Guidance in identifying and assessing the risks of proliferation financing.**

53. Regulations 18 **and 18A** states that in carrying out your risk assessment there are certain factors that you must take into account:

(i) any relevant information identified by your supervisory authority in relation to the risks of money laundering and terrorist financing (pursuant to reg. 17(9) and reg. 47) **and information in relation to proliferation financing identified by the Treasury (pursuant to reg. 18A(2)(a)**), i.e. supervisory **and Treasury** reports and risk assessments, in relation to which **by way of example** see [27] above.

(ii) risk factors specific to your practice (regs. 18(2)(b) **and 18A(2)(b)**) including factors relating to:

(a) your client;

(b) the country or geographic area in which you are practising;

(c) the service that you are providing;

(d) the relevant transaction; and

(e) the delivery channels through which your service is being provided ~~(reg. 18(3))~~;

54. You must keep an up-to-date written record of all steps taken in carrying out the risk assessment, and provide this, together with the risk assessment and any information on which that assessment was based, to your supervisor on request (reg. 18(4) & (6) **and 18A(4) and (5)**).

A Risk-Based Approach

61. The obligation in applying CDD under the Regulations is to do so on the basis of the risks of money laundering, ~~or~~ terrorist financing **or proliferation financing** as assessed by you in your risk assessment **taking into account the particular activity with the client**. To do this you should apply a sliding scale of risk assessment: the greater the perceived risk of money laundering, **terrorist financing or proliferation financing** the greater the extent of CDD measures that should be applied.

When must CDD be undertaken?

74. Where you are within the scope of the Regulations you must apply CDD when you:

(i) establish a business relationship,

(ii) carry out an occasional transaction that amounts to a transfer of funds above €1,000;

(iii) suspect money laundering or terrorist financing **and it would be prudent (not mandated) to do so if you suspect proliferation financing**; or

(iv) doubt the veracity or adequacy of documents, data or information previously obtained for the purpose of identification or verification (reg. 27).

76. In deciding whether it is an appropriate time to apply CDD to an existing client, you must take into account, among other things—

(i) any indication that the identity of the client, or of the client's beneficial owner, has changed;

(ii) any transactions which are not reasonably consistent you're your knowledge of the client;

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

(iv) any other matter which might affect your assessment of the money laundering or terrorist financing risk in relation to the client (reg. 27(9)) **and it would be prudent (not mandated) to do so if any other matter which might affect your assessment of the proliferation financing risk in relation to the client**.

78. Save for where the re-application of CDD is mandatory, the decision as to when CDD should be applied to an existing client must be fact specific and risk based (reg. 27(8)(a)). For example, it would not usually be necessary to re-apply CDD where a partner in a law firm who has instructed you in the recent past, on behalf of the same firm, wishes to instruct you again in relation to a low-risk matter on behalf of the same client. You should keep a record that a risk-based approach was taken and that due to the existing relationship and the low-level of money laundering/terrorist financing**/proliferation financing** risk, fresh CDD measures did not need to be applied.

Requirement to Report Discrepancies in Registers

88. **You must collect an excerpt of the register which contains certain details held on the register before the business relationship is established, or (if unavailable) must establish the information from an inspection of the register, in relation to:**

(i) ~~Before establishing a business relationship with~~ a company **(subject to the people with significant control requirements of Part 21A of the Companies Act 2006)**;

(ii) ~~(registered or~~**an** unregistered **company** (as defined in the Unregistered Companies Regulations 2009 (SI 2009/2436));

(iii) a Limited Liability Partnership **(subject to the Limited Liability Partnerships (Application of Companies Act 2006) Regulations 2009)**;

(iv) ~~or~~ a Scottish Partnership **(subject to the Scottish Partnerships (Register of People with Significant Control) Regulations 2017)**;

(v) a Trust **(subject to registration under Part 5 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017); or**

(vi) an overseas entity **(subject to registration under Part 1 of the Economic Crime (Transparency and Enforcement) Act 2022)** ~~which is required to register with HMRC's Trust Register or an overseas entity that needs to register due to ownership of UK real property you must collect proof of registration or an excerpt of the register from the company, the unregistered company, or the limited liability partnership (as the case may be) or from the registrar (in the case of an eligible Scottish partnership) - reg. 30A(1) an excerpt of the register which contains full details of any~~

~~information specified in paragraph (1A) (i.e. information relating to beneficial owners of the customer or where a registered overseas entity – information relating to registerable beneficial owners specified under Schedule 1 to the Economic Crime (Transparency and Enforcement) Act 2022) which is held on the register .~~

The details for an overseas entity (set out above in this paragraph) are the registrable beneficial owners specified in Schedule 1 to the Economic Crime (Transparency and Enforcement) Act 2022 and in respect of all of the other entities (set out above in this paragraph) this is information relating to beneficial owners of the client ~~at that time, or must establish from inspection of the register that there is no such information held on the register at that time~~.

87. ~~The proof of registration must include information relating to their beneficial owners, and where the customer is an overseas entity registering ownership of UK property, the beneficial owners they are required to register under the Economic Crime (Transparency and Enforcement) Act 2022.~~ **The information obtained must be updated whenever you are undertaking ongoing monitoring or refreshing due diligence on your client.** When undertaking this process you must report to the relevant registrar any material discrepancy that you find as between information relating to the beneficial ownership of the client and the register (reg. 30A(2)). You are not required to check for or report discrepancies involving existing ~~customers~~ **clients**.

88. Material discrepancies should be reported to Companies House (via the online reporting tool available on the Companies House website) **or HMRC in the case of trusts** as soon as reasonably possible. Examples of non-material discrepancies are given at 12.6 of the Part 1 Guidance and further information regarding the duty to report discrepancies **and how to make a report** has been provided by the government (available here).

93. Furthermore, you need to consider whether any unexplained or odd behaviour or aspects of the client's ongoing business activity give grounds for suspicion of money laundering, ~~or~~ terrorist financing **or proliferation financing**. In particular, you should consider the following on an ongoing basis:

(i) What is the commercial rationale for the transaction and does it make sense?

(ii) Are the client's funds for the transaction coming from a legitimate source?

(iii) Does the documentation make sense?

(iv) Have there been any unexpected developments or occurrences on the transaction?

(v) Do the instructions make sense in relation to what you already know about your client?

94. Where your ongoing monitoring leads you to consider that you have reasonable grounds to suspect money laundering, ~~or~~ terrorist financing **or proliferation financing** then you must comply with your obligations in relation to Suspicious Activity Reports.

Simplified Due Diligence

Application

97. Where you are entitled to apply simplified CDD measures, you must:

(i) continue to comply with the requirements of CDD (reg. 28) but you are entitled to adjust the extent, timing or type of CDD measures that you undertake to reflect your determination of a low risk of money laundering and terrorist financing **and you may consider whether it is prudent (not an entitlement) to do so in adjusting the extent, timing or type of CDD measures that you undertake to reflect your determination of a low risk of proliferation financing**; and

(ii) carry out sufficient monitoring of any business relationships or transactions which are subject to those measures to enable you to detect any unusual or suspicious transactions (reg. 37(1)).

Requirements

98. You may apply simplified CDD measures in relation to a particular business relationship or transaction where you determine that the business relationship or transaction presents a low degree of risk of money laundering, ~~or~~ terrorist financing **or proliferation financing**, having taken into account:

(i) the risk assessment you carried out in respect of your practice under Regulation 18(1) **and 18A(1)**; and

(ii) any relevant information identified by your supervisory authority in relation to the risks of money laundering and terrorist financing (pursuant to reg. 17(9) and reg. 47), i.e. supervisory reports and risk assessments, in relation to which see [27] above.

Low Risk Situations: Mandatory Risk Factors:

100. When assessing whether there is a sufficiently low degree of risk of money laundering, ~~or~~ terrorist financing **or proliferation financing** so as to justify the application of simplified due diligence measures, you must take account of risk factors including, among other things:

(i) customer risk factors, for example whether the client is a public body or an individual resident in a geographical area of lower risk;

(ii) product, service, transaction or delivery channel risk factors, for example whether the product or service is a low value life insurance policy or a low risk pension scheme or child trust fund;

(iii) geographical risk factors, for example whether the country where the client is resident is the UK or a third country which has been identified by credible sources, such as the Financial Action Task Force, the International Monetary Fund, the World Bank or the OECD as having effective systems to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016 and effectively implements those Recommendations.

NB:- You should refer to reg. 37(3) for the full list of mandatory risk factors.

101. In making the assessment referred to in reg. 37(3) above you must 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 **or proliferation financing** in a particular situation (**for example see** reg. 37(4)).

When Simplified Customer Due Diligence may no longer be applied

102. You must cease to apply simplified CDD measures where:

(a) you doubt the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification;

(b) your risk assessment changes and you no longer consider that there is a low degree of risk of money laundering, ~~and~~ terrorist financing **or proliferation financing**;

(c) you suspect money laundering, ~~or~~ terrorist financing **or proliferation financing**; or

(d) if any of the conditions set out in reg. 33(1) (the obligation to apply enhanced due diligence) apply (reg. 37(8)).

Enhanced Due Diligence

103. There may be circumstances in which it is appropriate to apply an 'enhanced' level of CDD than would normally be required. The risk of money laundering, ~~or~~ terrorist financing **or proliferation financing**, is variable in nature. Where there is an enhanced level of risk, an enhanced level of CDD should be applied to mitigate against the threat.

When enhanced due diligence must be applied

104. When carrying out CDD, reg. 33(1) requires that enhanced CDD measures, coupled with enhanced ongoing monitoring, must be applied in the following circumstances:

(i) in any case identified as one where there is a high risk of money laundering, ~~or~~ terrorist financing **or proliferation** either:

  (a) in the risk assessment carried out by you in respect of your practice (pursuant to reg. 18(1) **or 18A(1)**), or

  (b) in information made available to you by the relevant supervisory authority i.e. the BSB, Bar of NI or the Faculty of Advocates (pursuant to reg. 17(9) and 47);

(ii) 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;

(iii) in relation to correspondent relationships with a credit institution or a financial institution (in accordance with reg. 34);

(iv) if you have determined that a client or potential client is a PEP or a family member or known close associate of a PEP (in accordance with reg. 35);

(v) in any case where you discover that a client has provided false or stolen identification documentation or information and you propose to continue to deal with that client;

(vi) 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 (reg. 33(1)(f)),

and

(vii) In any other case which by its nature can present a higher risk of money laundering, ~~or~~ terrorist financing **or proliferation financing** (**for example see** reg. 33(1)(g)).

High Risk Situations: Mandatory Risk Factors

105. The Regulations require you to identify where there is a high risk of money laundering, ~~or~~ terrorist financing **or proliferation financing** (**for example see** reg. 33(1)(a)). When assessing the level of risk in such a situation, and the extent of the measures which should be taken to manage and mitigate that risk, reg. 33(6) states that you must take account of risk factors including, among other things:

(i) customer risk factors, for example where the business relationship is conducted in unusual circumstances, where the client is resident in a geographical area of high risk, the beneficiary of a life insurance policy, or where the client is a legal person or legal arrangement that is a vehicle for holding personal assets (e.g. a trust);

(ii) product, service, transaction or delivery channel risk factors, for example where the product involves:

  (a) private banking;

  (b) non-face-to-face business relationships or transactions, without certain safeguards, such as an electronic identification process which meets the conditions set out in reg. 28(19);

  (c) there is a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or other items of archaeological, historical, cultural or religious significance or of rare scientific value;

(iii) geographical risk factors, for example, countries:

  (a) that do not have effective systems to counter money laundering or terrorist financing or have significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;

  (b) providing support for terrorism;

  (c) identified by credible sources, such as the Financial Action Task Force, the International Monetary Fund, the World Bank or the OECD as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in June 2019.

NB:- You should refer to reg. 33(6) for the full list of mandatory risk factors.

106. In making the assessment referred to in reg. 33(6) above you must 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 **or proliferation financing** in a particular situation (**for example see** reg. 33(7)).

Persons Who Cease to be a PEP: ongoing monitoring

120. Where a person who was a PEP is no longer entrusted with a prominent public function, you must continue to apply the requirements in regs 35(5) and (8) in relation to that person either:

(i) for a period of at least 12 months after the date on which that person ceased to be entrusted with that public function; or

(ii) for such longer period as you consider appropriate to address the risk of money laundering, ~~or~~ terrorist financing **or proliferation financing** in relation to that person (**for example see** reg. 35(9)).

Professional Clients and Other Intermediaries

134. Where you are unable to complete CDD satisfactorily, you cannot accept or proceed with your instructions (reg. 31(1)). Where you **know, or suspect or** have reasonable grounds **for knowing or** ~~to~~ suspect**ing** that money laundering **(including proliferation financing)**, or terrorist financing is taking place you are also obliged to make a SAR.

138. You are also required to continue to monitor your relationship with your professional client for risks of money laundering, ~~or~~ the financing of terrorism **or proliferation financing**. That monitoring must be carried out using a risk-based approach. You also remain subject to the statutory obligations to report any suspicion of money laundering **(including proliferation financing)** or terrorist financing.

Public Access Cases

147. Should the relationship between your client and the intermediary alter in such a way as to make you consider that the intermediary has become the source of your instructions or has replaced your original client, you will need to address the altered situation. First, you will need to consider whether it is appropriate for you to continue to act. If you consider it appropriate to continue, you should then apply the required risk-sensitive CDD measures to the intermediary. If those measures are satisfied and you continue to act, thereafter you should continue to monitor your relationship with the client and, applying a risk-based approach, comply with your statutory obligations to report any **knowledge or** reasonable suspicions of money laundering **(including proliferation financing)** or terrorist financing to the NCA.

Suspicious Activity Reports

173. As the UKFIU, the NCA receives and analyses SARs concerning suspected proceeds of crime in order to combat money laundering, ~~and~~ terrorism **and proliferation financing**, and makes them available to law enforcement agencies for appropriate action.

*Compliance with Professional AML/CTF**/CPF** Guidance*

217. In deciding whether a person has contravened a relevant requirement, the "designated supervisory authority" must consider whether at the time the person followed ~~any relevant guidelines issued by the European Supervisory Authorities; Compliance with Professional AML/CTF/CPF Guidance~~ any relevant guidance which was at the time issued by the FCA, any other supervisory authority or appropriate body and approved by the Treasury, e.g. this Guidance (reg. 76(6)).

*Compliance with Professional AML/CTF**/CPF** Guidance*

224. In deciding whether a person has committed an offence under reg. 86(1), the court must decide whether that person followed:

~~(i) any guidelines issued by the European Supervisory Authorities;~~

~~(ii)~~(i) any relevant guidance which was at the time issued by the FCA, supervisory authority or appropriate body and approved by the Treasury, e.g. the Legal Sector AML Guidance (reg. 86(6)).

Annex 1 - A Basic Guide to Customer Due Diligence

A. Individual

A person with whom you have a direct relationship.

Identification

1. Full name

~~2.~~ Residential address (including country of residence) **or**

2. Date of Birth, and

3. Country of citizenship

C. Listed entity

Control and ownership

For entities listed on an Unregulated Market or Exchange list, if the entity claims that it does not have UBOs of 25% or more, its ownership should still be understood along with the source of funds (which may be apparent from the nature of the entity).

Obtain understanding of the overall control and ownership structure and verify information according to risk categorization.