BRITISH ART MARKET FEDERATION

GUIDANCE ON ANTI MONEY LAUNDERING

For UK Art Market Participants

APPROVED BY HM TREASURY

24 JANUARY 2020

BRITISH ART MARKET FEDERATION

GUIDANCE ON ANTI MONEY LAUNDERING

For UK Art Market Participants

PART I - OVERVIEW

APPROVED BY HM TREASURY

24 JANUARY 2020

https://tbamf.org.uk/

INTRODUCTION

Offences in relation to money laundering have been in place – and have applied to art market participants - for many years under the Proceeds of Crime Act 2002 (POCA). From 10 January 2020 art market participants who deal in sales, purchases and/or storage of works of art (as defined in s21(6) of the VAT Act 1994) with a value, for a single transaction or a series of linked transactions, of 10,000 euros or more, will be subject to further anti money-laundering obligations, under the Money Laundering Regulations 2017.

A number of other industry sectors, such as banking, have long been the subject of an anti-money laundering regulatory framework. The reason for now extending that framework to the art market is a concern that the art market could be used by criminals to launder the proceeds of crime such as drug trafficking, modern slavery, tax evasion, corruption or theft.

At the heart of the new Regulations is a requirement that art market participants must identify the physical person who they are dealing with in any transaction or, when dealing with a corporate body or a trust, the person or persons who control that entity. In other words, "Who are you *really* dealing with?" This is known as customer due diligence (CDD).

Any person or entity identified in this way will also be required to verify and prove their identity, either through identity documents or official corporate documents, or electronically.

Commercial and personal confidentiality are an important feature of the art market, and for good and valid reasons. However, these new rules are designed to limit the risk of confidentiality being abused in order to hide illicit activity. While confidentiality and discretion will continue to be a feature of the art market, the changes introduced by the new regulations may in some cases result in a degree of increased transparency between art market participants.

Supporting the requirement to ascertain and verify identity is a regulatory structure. Art market participants who deal in sales, purchases and/or storage of works of art with an individual value, for a single transaction, or a series of linked transactions of 10,000 euros or more will be required to register with HMRC, put in place anti money laundering processes, nominate a person responsible for anti-money laundering compliance, train staff, report suspicions and keep records. Compliance with these requirements may be checked by HMRC through a range of compliance activity.

This guidance document, produced by the British Art Market Federation and approved by HM Treasury, is designed to provide a detailed explanation of the new requirements. It is however merely guidance and is not intended to be a substitute for legal advice. The guidance document is divided into two parts. The first – Part 1 - is a general overview of the legislation and will answer many of the more general questions art market participants may have about whether they fall within the scope of the new regulations and what they need to do to comply. The second – Part II – is designed to provide a more comprehensive analysis of the Regulations addressing some of the more detailed aspects of the requirements.

Purpose of these guidelines

1. The EU Fifth Money Laundering Directive (5MLD) introduced changes which bring art market participants into the scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[1] ('ML Regulations') from 10 January 2020[2]. Art businesses have long had legal obligations to prevent and report suspected money laundering under the Proceeds of Crime Act, irrespective of the value of the transactions they engage in. These obligations continue, but extended obligations are imposed by the ML Regulations on art market participants, which are subject to regulatory supervision, oversight and enforcement by HMRC, and this practical guidance should help firms to implement the requirements of the Regulations.

2. The changes introduced mean that from 10 January 2020, art market participants (AMPs) as defined in the Regulations must:

    - Register with HMRC before they carry on with their business, where this involves a transaction of 10,000 euros or more, or a series of linked transactions of 10,000 euros or more
    - Carry out a risk assessment of the extent to which they are exposed to money laundering
    - Carry out customer due diligence measures on customers *before* they conclude a transaction;
    - Appoint a nominated officer
    - Maintain a prescribed range of policies, controls and procedures
    - Train staff appropriately
    - Report suspicious transactions to the authorities
    - Keep appropriate records of customer due diligence and of transactions

3. This guidance, which comprises two parts, namely an Overview (Part I) and more comprehensive Guidelines with source references to the ML Regulations (Part II), sets out the requirements of the relevant law and regulations and how they may be implemented in practice.

Who are the guidelines addressed to?

4. The Guidelines, prepared by BAMF members and formally approved by HM Treasury, are addressed to those art market participants (AMPs) as defined by the ML Regulations, represented by it and by its member bodies. AMPs who are neither members of BAMF nor of its member trade associations should have regard to the Guidelines as industry good practice. The detailed obligations, considerations and examples set out in Part II in particular, will be of direct relevance to senior management and nominated officers of firms.

Meanings and definitions

What is money laundering and what are the proceeds of crime?

[1] http://www.legislation.gov.uk/uksi/2017/692/made

[2] http://www.legislation.gov.uk/uksi/2019/1511/contents/made

5. Money laundering is defined in section 340 of the Proceeds of Crime Act 2002 (POCA) and covers wide ranging circumstances involving any activity concerning the proceeds of any crime. Money laundering takes many forms, including:
    - trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);
    - possessing or transferring the benefit of crimes such as tax evasion, fraud and theft;
    - possessing or transferring stolen goods;
    - being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
    - criminals investing the proceeds of their crimes in the whole range of artworks.

6. Broadly, the term 'proceeds of crime' or 'criminal proceeds' refers to all property from which a person benefits directly or indirectly, by being party to criminal conduct, for example, money from corruption, embezzlement, drug dealing or stolen (such funds are commonly referred to as criminal property). It also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a work of art. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer wishes to operate.

7. There are three broad groups of offences related to money laundering that firms need to avoid committing. These are:
    - knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
    - failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
    - tipping off, or prejudicing an investigation.

8. It is also a separate offence under the ML Regulations not to establish adequate and appropriate policies and procedures in place to forestall and prevent money laundering (regardless of whether or not money laundering actually takes place).

Money laundering in the AMP sector

9. Offences in relation to money laundering have been in place for many years, under POCA. In the art market, money laundering risks can arise in relation to the sale or the purchase of a work of art.

10. On the selling side, there is a risk that an AMP handles or facilitates a sale of a work of art which is stolen, looted or purchased with the proceeds of crimes such as tax evasion, fraud, forgery, bribery/corruption, illegal trade in stolen goods, insider trading, market abuse, drug trafficking. There is also a risk it is linked to terrorist financing.

11. On the buying side, money laundering could occur where the AMP facilitates the purchase of a work of art with funds which are derived from criminal activities.

Examples:

- An art dealer sells a sculpture and pays the net proceeds of sale to the ultimate seller. Had the dealer, prior to the sale, carried out a lost/stolen art database check, she would have discovered that the sculpture had been stolen in a high profile theft from a museum.
- A buyer purchases a high value painting from an art dealer at a major art fair. Payment for the painting is received into the dealer's bank account from an offshore bank account and the painting is promptly collected. Customer due diligence checks would have discovered that the buyer was actively being investigated for tax evasion and money laundering and that the laundered proceeds of his crimes were reportedly held at the bank from which payment was received.
- The wife of an art collector who has been recently been sentenced to imprisonment for a long history of insider dealing buys a painting at auction. Funds are wired to the auction house from a Panamanian entity owned solely by the art collector. The auction house accepts the funds, releases the painting to the collector's wife and pays the vendor. There is a risk that the auction house has accepted criminally derived funds and facilitated money laundering.

Who is an "art market participant", and what is the scope of regulated activity in the context of an art transaction?

12. An art market participant is defined in the ML Regulations as

'a firm or sole practitioner who

(i) by way of business trades in, or acts as an intermediary in the sale or purchase of, works of art and the value of the transaction, or a series of linked transactions, amounts to 10,000 euros or more; or

(ii) is the operator of a freeport when it, or any other firm or sole practitioner, by way of business stores works of art in the freeport and the value of the works of art so stored for a person, or a series of linked persons, amounts to 10,000 euros or more.'

What is a "work of art?"

13. A work of art is as defined in s21 of the Value Added Tax Act 1994. S21(6) in particular sets out the definition – see Annex I. It should be noted that antiques (such as furniture, early automobiles etc.) and collectors' items (such as coins, ethnographic items and stamp collections) are not within this definition, although conceptual works of art would fall within the definition.

Overview

14. This Overview gives high level guidance on the requirements set out in the ML Regulations, which are more fully detailed in Part II. It covers -

- Responsibilities of senior management
- Application of requirements to art market participants
- Requirement to register with HMRC
- Requirement to follow a risk based approach and prepare a risk assessment

- Obligation to appoint a nominated officer
- Requirements for policies, controls and procedures
- Training
- Obligation to carry out customer due diligence
- Obligation to report suspicions
- Obligation to keep records

Responsibilities of senior management

15. Senior management are officers or employees, with sufficient knowledge of the business's money laundering and terrorist financing exposure, who have authority to make decisions affecting the firm's exposure to money laundering and terrorist financing. Examples include the chief executive, owner, director, manager, company secretary, a sole proprietor or a partner in a partnership.

16. It is the responsibility of senior management to decide on and to guide the risk based approach, approve the AMP's policies, controls and procedures for mitigating the risks identified in the risk assessment, appoint a nominated officer to report suspicious activity to the National Crime Agency and devote sufficient resources to implement policies, controls and procedures effectively. Senior management are also responsible for ensuring and monitoring compliance throughout the firm (including by subsidiaries, branches and agents).

17. Senior management can be held personally liable if they fail in these responsibilities.

Application of requirements to art market participants

18. An AMP conducts regulated activity under the ML Regulations if it deals, as defined in the ML Regulations, in works of art with an invoiced value of 10,000 euros or more. Only those AMPs which engage in regulated activities are subject to the requirements of the ML Regulations and to the obligation to register with HMRC. Trade in antiques (such as furniture, early automobiles etc.) and collectors' items (such as coins, ethnographic items and stamp collections) are not subject to the requirements of the ML Regulations (unless cash payments of 10,000 euros or more are involved). For those AMPs which engage in a mixture of regulated and unregulated transactions, the ML Regulations will apply to the regulated transactions only. The internal risk assessment of such AMPs should clearly state which part of their business activities are regulated.

19. It is important to note that the obligation under the ML Regulations to carry out CDD measures applies to those AMPs which carry out transactions with 'customers' to whom the obligation applies – see paragraph 47 below. All AMPs are subject to obligations under POCA (including additional obligations because AMPs are now in the regulated sector – see paragraphs 6.15, 6.18 and 6.34 in Part II below), which apply in respect of all activity that their business undertakes.

20. For a firm to remain outside the scope of the ML Regulations it would be important for it to be clear, as a matter of policy, on whether it deals, or is likely to deal, in sales of works of art over 10,000 euros.

How is the 10,000 euros limit calculated?

21. The value of a work of art sold at public auction is the hammer price including taxes, commission and ancillary costs. The value of a work of art sold commercially through any other means is the final invoiced price for the work of art including taxes, commission and ancillary costs.

22. The 10,000 euros limit applies to linked transactions totalling 10,000 euros or more, or where the transaction appears to be deliberately broken down into several payments below 10,000 euros. HMRC considers multiple payments against a single invoice, which together exceed the 10,000 euros threshold, to be linked, regardless of how long it takes to make payment.

Requirement to register with HMRC

23. Under the ML Regulations, HMRC is designated as the supervisory authority for AMPs. All AMPs presently falling within scope of the ML Regulations need to register with HMRC. AMPs who are within scope must register before 10 January 2021.

24. Although AMPs falling within scope are strongly advised not to delay submission of registration applications in the period between 10 January 2020 and 9 January 2021 inclusive, they may continue to undertake transactions of 10,000 euros or above without having applied for registration during that period. However, irrespective of whether or not they have yet registered with HMRC, from 10 January 2020 they must carry out due diligence on all customers to whom they sell works of art at 10,000 euros or above, and must meet the other obligations imposed on the sector under the ML Regulations.

25. From 10 January 2021, AMPs who will be conducting transactions that will bring them within scope of the ML Regulations, must immediately apply to HMRC for registration. They may, however, proceed with any transactions within scope of the Regulations whilst awaiting confirmation that their registration has been approved, provided they are meeting all their other obligations under the ML Regulations.

26. In the case of transactions that unexpectedly bring a firm within scope, the firm should apply for registration as soon as practicable after any relevant transactions have occurred. If an unregistered AMP undertakes an unexpected and isolated occasional transaction, they should adhere to the requirements of the regulations and should seek the advice of HMRC immediately (MLRCIT@hmrc.gsi.gov.uk) Overseas dealers coming to the UK to sell works of art fall into scope of Regulation 14(d)(i), and so need to register with HMRC.

27. Registration is via the HMRC weblink https://www.gov.uk/guidance/register-or-renew-your-money-laundering-supervision-with-hmrc. See also https://www.gov.uk/guidance/money-laundering-regulations-registration-fees.

28. As part of the process of registration, the beneficial owners and senior management of AMPs are subject to approval by HMRC to ensure that they are appropriate people to undertake their responsibilities.

Requirement to follow a risk based approach and prepare a risk assessment (see Part II – section 1 for further details)

29. AMPs should adopt a 'risk based approach' to preventing and detecting money laundering. This approach applies in two ways:

    - assessing the level of money laundering and terrorist financing risk to which the AMP is exposed by virtue of the nature of its business;

    - assessing the level of risk in a particular customer (i.e. on a day to day, customer by customer basis).

30. All AMPs undertaking regulated business should undertake and maintain a documented risk assessment. The risk assessment should assess the exposure of the AMP to the risk of money laundering and terrorist financing, and identify what mitigation is in place, or needs to be in place, e.g., policies, controls and procedures.

31. Relevant considerations for a risk assessment include the size and nature of the business, how often it engages in regulated activities, geographical risk, customer risk (including whether the AMP transacts with Politically Exposed Persons (PEPs)), channels of selling such as public auction, gallery, shops (face to face and on-line), private sales, and the type and value of works of art generally offered. Risk assessments should be documented and reviewed regularly, at least on an annual basis, and certainly following any significant changes in the AMP's business, to reflect changes in circumstances and the UK's latest national risk assessment, as well as any further information made available by HMRC.

32. The conclusions of the AMP's risk assessment are a matter of judgment and although there is no set method for documenting a risk assessment, it is important that the critical evaluation of all potential money laundering or terrorist financing risks is clearly demonstrated. Regulatory supervisors can ask to see a firm's risk assessment at any time, especially if something goes wrong.

33. The conclusions of the risk assessment should feature in the AMP's policies, controls and procedures and inform where resources should be focused. Those areas which carry the greatest risk of money laundering or terrorist financing should be carefully managed and monitored, while those areas determined to present a low risk may be subject to lighter touch risk mitigation and controls.

Obligation to appoint a nominated officer (see Part II – section 2 for further details)

34. All AMPs carrying out regulated activities under the ML Regulations must appoint a nominated officer of appropriate seniority within the business to receive reports of suspicious activity from staff and decide whether to report such knowledge or suspicions to the National Crime Agency. AMPs should appoint a deputy to act in the absence of the nominated officer. The nominated officer and deputy should have access to all client files, accounting records and other relevant information, sufficient to enable them to make independent decisions and to liaise with law enforcement.

35. A sole trader with no employees will be the nominated officer of a firm.

36. Larger, more complex firms (for example, those which carry out regulated activities from multiple premises through numerous employees, or have a high number of transactions involving foreign customers and intermediaries, or who do business via multiple sales channels) must also appoint a compliance officer to ensure compliance with the Regulations. HMRC would not expect a small firm with few employees, an uncomplicated business model and few regulated transactions to have a dedicated compliance officer.

37. The role of a compliance officer would include ensuring that the AMP firm is compliant with the regulations and that policies and procedures are consistently complied with throughout the firm. Their responsibilities might also include conducting audits to test adherence to policies, procedures and controls and implementing improvements following such reviews.

38. HMRC expects the nominated officer, and any deputy, to be based in the UK.

Requirements for policies, controls and procedures (see Part II – section 3 for further details)

39. An AMP's policy statement should set out in writing the commitment and responsibilities of senior management and all employees in relation to implementing an effective anti-money laundering regime. Policies and procedures must be relevant and proportionate to the size and nature of the business and kept under regular review.

40. An AMP's policies and procedures must include:

- The risks of ML/TF identified in the risk assessment
- The responsibilities of senior management and all employees in relation to anti-money laundering compliance
- Customer due diligence measures – including identification and verification requirements, identification of customers or beneficial owners who are Politically Exposed Persons (PEPs) or family members or close associates of PEPs, timing of customer due diligence and the exercise of discretion on risk based aspects
- Suspicious activity reporting procedures
- Internal control procedures, including cash and third party payment handling
- Use of reliance or outsourcing arrangements
- Ongoing monitoring activities

Training (see Part II – section 4 for further details)

41. Even the best designed anti-money laundering regimes in an AMP firm can be quickly compromised if the employees who deal with customers, payments, due diligence in respect of works of art and any compliance aspects, or representatives of the AMP, are not adequately trained.

42. Delivery of staff training should be carried out in a clear and effective way, and repeated sufficiently often, including when new employees join the firm, when roles change, or when regulations, policies or procedures change. Training may be provided by internal or external compliance experts in many formats, including face-to-face, on-line or via seminars and conferences.

43. The type of training given should be appropriate to specific employees, so that they are properly equipped to deal with the particular risks that they come across when fulfilling their responsibilities. For example, client-facing staff registering or dealing with new clients should be trained on conducting client due diligence checks, including awareness of the possibility of forged documents. Those handling payments should be trained to identify third party payments and red flags (for more information on red flags, see Part II, paragraphs 4.21-4.22) relating to the origin of funds. All employees should be trained on how to spot red flags and on the obligation to report suspicions to the AMP's nominated officer.

44. AMPs should maintain records of training and may be asked to produce evidence of training to HMRC.

Obligation to carry out customer due diligence ['CDD'] measures (see Part II – section 5 for further details)

45. CDD measures should enable AMPs to form a reasonable belief that they know the true identity of each customer and, where relevant, their beneficial owner (that is, the person or entity who owns or exercises ultimate control over the customer, or on whose behalf a transaction is being undertaken). The ML Regulations require an AMP to identify the customer, verify the identity, and assess the purpose and intended nature of the business relationship or occasional transaction.

46.AMPs engaging in regulated activity must apply CDD measures when -

- establishing a business relationship with a customer (see paragraph 56)
- carrying out an occasional transaction -
  - in relation to the trade of a work of art (within the meaning given in regulation 14), when they carry out, or act in respect of, any such transaction, or series of transactions, whose value amounts to 10,000 euros or more
  - in relation to the storage of a work of art (within the meaning given in regulation 14), when it is the operator of a freeport and the value of the works of art so stored for a person, or series of linked persons, amounts to 10,000 euros or more
- they suspect money laundering or terrorist financing, irrespective of the value of the transaction or
- they doubt the veracity of documents or information previously obtained for the purpose of identification or verification.

Who is the customer for CDD purposes? (Part II, paragraphs 5.5 – 5.19)

47. The "customer" for the purposes of the ML Regulations will vary, depending on the AMP's business model. It will be the purchaser of a work of art, and any broker or agent acting for them. It will be the seller, where the AMP provides a service to, and receives financial value from, them.

48. The AMP conducting the transaction must apply CDD measures to the customer, so that they can identify the customer and, where necessary, the source of funds.

49. This is in addition to an AMP's continuing obligations under POCA (and additional obligations because the AMP is now in the regulated sector – see paragraphs 6.15, 6.18 and 6.34 in Part II) to ensure that they have no reasonable suspicion that they are handling or facilitating a sale of a work of art which itself represents the proceeds of crime. They also have obligations under UK and EU sanction regimes to ensure that they are not dealing or transacting with any sanctioned person. To meet POCA and sanctions obligations, therefore, it may be appropriate (as determined on a risk-based approach) for an AMP to carry out further checks on the seller or consignor of a work of art, to ensure that they are not handling stolen works of art, or otherwise facilitating use of the proceeds of crime.

50. An AMP in the trade of a work of art has an obligation to carry out CDD on its customer and on any ultimate beneficial owner of the customer.

51. Where a customer is acting as an agent, the AMP conducting the transaction has an obligation under the ML Regulations to carry out CDD on the agent and also on the ultimate customer, as the AMP must know the identity of the person who is ultimately paying for the work of art. The AMP must also verify that the agent is authorised to act on behalf of the customer. An AMP acting as a selling agent has an obligation to carry out CDD on the person on whose behalf they are selling the artwork. The buyer, or his agent, however, has no obligation or right to know the identity of the ultimate seller.

*Reliance (Part II – paragraphs 5.190-5.212***)**

52. An AMP conducting a transaction is obliged under the ML Regulations to know the identity of their customer (and ultimate beneficial owner as described and defined in paragraph 45 above). However, to avoid duplication of effort the ML Regulations specifically permit AMPs to rely on CDD measures conducted by other AMPs who are subject to the requirements of the ML Regulations or equivalent. Therefore, by way of example, an auction house may choose to rely on a regulated agent to have collected the relevant customer due diligence documentation on the customer that the agent is representing at an auction. However, it is important to be aware that the relying AMP conducting the sale retains responsibility, and is liable for any failure to comply with the CDD obligations set out under the ML Regulations, as this responsibility cannot be delegated. The relying AMP should therefore assess whether it has confidence that the intermediary or agent will have carried out CDD measures appropriately, and should obtain written assurances to this effect (see paragraph 5.206).

CDD measures (Part II – paragraphs 5.20ff)

53. An AMP must assess whether there are any 'red flags' in relation to a particular customer. Where an AMP has made an assessment and determined that there are no 'red flags' and the money laundering risk in relation to a particular customer is low, the AMP will apply standard customer due diligence. On the other hand, where the AMP's assessment shows that there are 'red flags' and a particular customer presents a higher risk of money laundering (or is in a category, such as a politically exposed person, where the ML Regulations specifically require enhanced due

diligence), additional customer due diligence measures must be undertaken. (For more information on red flags, see Part II, paragraphs 4.21-4.22)

Timing of carrying out CDD measures

54. In general, CDD must be completed prior to the completion of a transaction and this would normally be the case in relation to the sale of an artwork. This means, for example, where a dealer at an art fair makes a sale to a new customer, a transaction may be agreed ahead of carrying out all required CDD measures, but CDD measures are to be completed before release of the work of art to the customer. Likewise, for auctions, it may not be possible to apply CDD measures to every bidder who registers to bid immediately prior to a sale, but CDD measures must be applied to the successful bidder prior to completion of the transaction, that is, before the work of art is released to the successful bidder.

55. Where the nature of a delay in providing CDD information suggests that the customer is deliberately being evasive, or there are other reasons that constitute 'red flags', the AMP should consider whether to enter into the transaction with the customer at all and determine whether to make a suspicious activity report.

Customer relationships/updating CDD/monitoring

56. A business relationship in the art market is a business, professional or commercial relationship between a business and a customer, which the business expects, on establishing the contact, to have an element of duration. For example, a business relationship for a business might exist where:

- there is a contract to provide regular services
- customers have extended credit terms arrangements or financing or loan arrangements
- a buyer asks a dealer to source multiple paintings of a particular kind for their art collection over a period of time

57. The majority of transactions in the art market are, however, likely to be occasional, on the basis that there is no obligation or commitment on the customer to use services or buy goods again, or form an ongoing relationship with the AMP. Receiving marketing materials or attending events, such as gallery openings does not constitute a "business relationship" for ML Regulation purposes.

58. AMPs will therefore need to exercise judgement as to with which customers, if any, they have a business relationship, and which customers come to them only for an occasional transaction.

59. There are some additional provisions under the ML Regulations in relation to customers with whom an AMP has a business relationship.

- There is an obligation to monitor the activity of customers with whom the AMP has a business relationship. The activity should be consistent with the AMP's knowledge of the customer. [Monitoring is not required for customers who only carry out occasional transactions with the AMP.]

- In relation to such customers, an AMP is required to keep customer information up to date, and so should be alert to changes which may trigger a need to bring the customer due diligence up to date.

Obligation to report suspicions (see Part II – section 6 for further details)

60. The nominated officer must make a report to the National Crime Agency (NCA) in respect of information that comes to them within the course of business where they *know* or *susp*ect or *have reasonable grounds for knowing or suspecting* that a person is engaged in, or attempting, money laundering or terrorist financing – even if no transaction goes ahead.

61. Reports must be made to the NCA as soon as it is practical to do so. For suspicious activity reports known as 'defence against money laundering', where consent is requested from the authorities in order to proceed with a transaction, no transaction should take place until consent is received. The process for reporting suspicions is detailed in Part II – section 6.

62. It is a criminal offence for an employee of the AMP to do or say anything that 'tips off' another person that a disclosure has been made to the NCA where the tip-off is likely to prejudice any investigation that might take place. AMPs should alert their staff to the personal liability that attaches to passing on such information.

Obligation to keep records (see Part II – section 7 for further details)

63. AMPs must maintain appropriate systems for retaining records and making records available when required within specified timescales. The following must be retained:

    - copies of evidence obtained to satisfy CDD obligations and details of customer transactions for at least five years after the end of the business relationship
    - details of occasional transactions for at least five years from the date of the transaction
    - details of actions taken in respect of internal and external suspicion reports
    - details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make a suspicious activity report
    - copies of the evidence obtained if the AMP is relied on by another person to carry out CDD, for five years from the date that the other person's relationship with the AMP ends.

Status of these guidelines

64. The Proceeds of Crime Act (POCA), the Terrorism Act 2000 and the ML Regulations all provide that when deciding whether a person or firm has committed an offence under the relevant law or regulation, a court must decide whether that person or firm followed relevant Treasury-approved industry guidance.

65. These guidelines, approved by a Treasury Minister, therefore provide a sound basis for AMPs in the UK art market to meet their legislative and regulatory obligations, when applied by them to their particular business risk profile. Following the guidance offered is not mandatory, although departures from these guidelines, and the rationale for so doing, should be documented,

and AMPs may have to stand prepared to justify departures, for example to HMRC and the courts.

How should the guidelines be used?

66. The guidelines set out in Part II provide more comprehensive guidance on how AMPs may take a risk based approach to how they comply with AML/CTF legislation and regulation, and on the procedures that they put in place for this purpose.

67. The guidelines are not intended to be a substitute for legal advice and nothing in them should be construed as such. Anyone requiring clarification on the legal issues contained in the guidelines should seek their own independent legal advice. Neither are the guidelines a substitute for AMPs' individual risk management plans. AMPs should refer to the Regulations and associated legislation in making decisions in relation to the Regulations. Any examples included in these guidelines are for illustrative purposes only.

68. AMPs should encourage their staff to 'think risk' as they carry out their duties. HMRC has a clear expectation that the firms they supervise address their management of risk in a thoughtful and considered way, and establish and maintain systems and procedures that are appropriate, and proportionate to the risks identified. These guidelines assist AMPs in doing this.

69. When provisions of the statutory requirements and of HMRC's regulatory requirements are directly described in the text of the guidelines, the term 'must' is used. In other cases, the guidelines use the term 'should', to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements. References to 'must' and 'should' in the text should therefore be construed accordingly.

Further sources of guidance

70. The Joint Money Laundering Steering Group (a group made up of trade associations in the financial services industry) also publishes free detailed guidance. That guidance is for members of the trade associations and firms supervised by the Financial Conduct Authority, for compliance with the ML Regulations. However, some of the sections in Part I of the JMLSG Guidance may be particularly relevant to AMPs. They contain detailed coverage of how to carry out due diligence checks on different types of customers, report suspicious activity and carry out staff training and record keeping.

- The Joint Money Laundering Steering Group publishes more information about businesses' obligations and the level of risk in other jurisdictions (Annex 4-1 of Part I) http://www.jmlsg.org.uk/
- The Financial Conduct Authority has published detailed guidance on the treatment of politically exposed persons (PEPs) for anti- money laundering purposes. Paragraphs 2.16 -2.18 of the FCA document describes who should be treated as a PEP.
- The National Crime Agency (NCA) has published guidance on making Suspicious Activity Reports (SARs) suspicious activity on their website: How to report SARs.

ANNEX I

EXTRACT FROM S21 OF VALUE ADDED TAX ACT 1994, as amended

MEANING OF 'WORK OF ART'

21 (6) In this section "work of art" means, subject to subsections (6A) and (6B) below—

(a) any mounted or unmounted painting, drawing, collage, decorative plaque or similar picture that was executed by hand;

(b) any original engraving, lithograph or other print which—

(i) was produced from one or more plates executed by hand by an individual who executed them without using any mechanical or photomechanical process; and

(ii) either is the only one produced from the plate or plates or is comprised in a limited edition;

(c) any original sculpture or statuary, in any material;

(d) any sculpture cast which—

(i)was produced by or under the supervision of the individual who made the mould or became entitled to it by succession on the death of that individual; and

(ii)either is the only cast produced from the mould or is comprised in a limited edition;

(e) any tapestry or other hanging which—

(i)was made by hand from an original design; and

(ii)either is the only one made from the design or is comprised in a limited edition;

(f) any ceramic executed by an individual and signed by him;

(g) any enamel on copper which—

(i)was executed by hand;

(ii)is signed either by the person who executed it or by someone on behalf of the studio where it was executed;

(iii)either is the only one made from the design in question or is comprised in a limited edition; and

(iv)is not comprised in an article of jewellery or an article of a kind produced by goldsmiths or silversmiths;

(h) any mounted or unmounted photograph which—

(i)was printed by or under the supervision of the photographer;

(ii)is signed by him; and

(iii)either is the only print made from the exposure in question or is comprised in a limited edition;

(6A) The following do not fall within subsection (5) above by virtue of subsection (6)(a) above, that is to say—

(a) any technical drawing, map or plan;

(b) any picture comprised in a manufactured article that has been hand-decorated; or

(c) anything in the nature of scenery, including a backcloth.

(6B) An item comprised in a limited edition shall be taken to be so comprised for the purposes of subsection (6)(d) to (h) above only if—

(a) in the case of sculpture casts—

(i)the edition is limited so that the number produced from the same mould does not exceed eight; or

(ii)the edition comprises a limited edition of nine or more casts made before 1st January 1989 which the Commissioners have directed should be treated, in the exceptional circumstances of the case, as a limited edition for the purposes of subsection (6)(d) above;

(b) in the case of tapestries and hangings, the edition is limited so that the number produced from the same design does not exceed eight;

(c) in the case of enamels on copper—

(i)the edition is limited so that the number produced from the same design does not exceed eight; and

(ii)each of the enamels in the edition is numbered and is signed as mentioned in subsection (6)(g)(ii) above;

(d) in the case of photographs—

(i)the edition is limited so that the number produced from the same exposure does not exceed thirty; and

(ii)each of the prints in the edition is numbered and is signed as mentioned in subsection (6)(h)(ii) above.

ANNEX II

SUMMARY OF CURRENT LEGISLATION

1. Money laundering law aims to prevent and detect the use of any proceeds of crime, and to prevent and detect terrorist financing. Businesses within the scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[3] ('ML Regulations'), which from 10 January 2020[4] will include art market participants, have a specific legal obligation to have policies, procedures and controls in place covering the risks they face from money laundering and terrorist financing.

2. The legal framework principally comprises the ML Regulations and the Proceeds of Crime Act 2002 ('PoCA'), in the context of the UK financial sanctions regime. Under the ML Regulations, businesses must establish and maintain appropriate systems and controls, carry out appropriate customer due diligence, require trained staff to report suspicions of money laundering and keep appropriate records. Under the Proceeds of Crime Act, businesses and staff (whether registered with HMRC or not) have a legal obligation not to deal, knowingly or unknowingly, in criminal property. Under the sanctions regime, firms must not enter into transactions or arrangements with specific, named individuals and entities.

3. The main pieces of UK legislation covering anti-money laundering and counter-financing of terrorism are:

   - Proceeds of Crime Act 2002
   - Terrorism Act 2000
   - Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)
   - Criminal Finances Act 2017
   - Terrorist Asset-Freezing etc. Act 2010
   - Anti-terrorism, Crime and Security Act 2001

   The Proceeds of Crime Act

   The Proceeds of Crime Act sets out the primary offences related to money laundering:

   - concealing, disguising, converting, transferring or removing criminal property from the UK
   - entering into or becoming involved in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
   - the acquisition, use and/or possession of criminal property.

   The primary money laundering offences apply to everyone.

   The Proceeds of Crime Act also creates offences of failing to make a report about suspicious activity, and tipping off any person that the firm has made, or intends to make, such a report.

[3] SI 2017/692
[4] http://www.legislation.gov.uk/uksi/2019/1511/contents/made

This applies to nominated officers and employees of businesses in the regulated sector, such as art market participants. This obligation extends across the whole business, so an art market participant should also report any suspicious activity irrespective of the value of the transaction.

The Terrorism Act

The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses, like art market participants, must report belief or suspicion of offences related to terrorist financing, such as:

- fundraising for the purposes of terrorism
- using or possessing money for the purposes of terrorism
- involvement in funding arrangements
- money laundering - facilitating the retention or control of money that's destined for, or is the proceeds of, terrorism.

The Criminal Finances Act 2017

The Criminal Finances Act 2017 extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism.

The ML Regulations

The Regulations set out what art market participants must do to prevent the use of their services for money laundering or terrorist financing purposes.

The Terrorist Asset-Freezing etc. Act 2010

The Terrorist Asset-Freezing etc. Act 2010 gives HM Treasury power to freeze the assets of individuals and groups reasonably believed to be involved in terrorism, whether in UK or abroad, and to deprive them of access to financial resources.

The Anti-terrorism, Crime and Security Act 2001

The Anti-terrorism, Crime and Security Act 2001 allows for freezing orders to be made against national security threats and the civil asset seizure regime for terrorism.

Financial sanctions

The Office of Financial Implementation (OFSI), which is part of HM Treasury, publishes a list of all those subject to financial sanctions imposed by the UK. OFSI helps to ensure that these financial sanctions are properly understood through sanction notices, guidance and news releases. All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

A firm must report to OFSI as soon as practicable if it knows or has reasonable cause to suspect that a designated person has committed an offence. The firm should report any transactions

carried out for persons subject to sanctions or if they try to use its services. A firm can report a suspected breach, sign up for free email alerts and obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:

https://www.gov.uk/government/organisations/office-of-financial-sanctionsimplementation

BRITISH ART MARKET FEDERATION

GUIDANCE ON ANTI MONEY LAUNDERING

For UK Art Market Participants

PART II: GUIDELINES

APPROVED BY HM TREASURY

24 JANUARY 2020

CONTENTS

BAMF GUIDELINES ON ANTI MONEY LAUNDERING

LIST OF ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	
AML	Anti-money laundering
CTF	Combating terrorism financing
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CTF standards, both at national and international levels
FCA	Financial Conduct Authority, the UK regulator of the financial services industry
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
MiFID	The Marketing in Financial Instruments Directive
ML Regulations	The Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017
MLRO	Money Laundering Reporting Officer
NCA	The National Crime Agency, the UK's financial intelligence unit.
POCA	Proceeds of Crime Act 2002
SAR	Suspicious activity report
PEP	Politically Exposed Person
CDD	Customer Due Diligence
SDD	Simplified Customer Due Diligence
EDD	Enhanced Customer Due Diligence
OFSI	Office of Financial Sanctions Implementation

GLOSSARY AND DEFINITIONS

Term/expression	Meaning
Art Market Participant	An art market participant is defined in the ML Regulations as *'a firm or sole practitioner who* *(iii) by way of business trades in, or acts as an intermediary in the sale or purchase of, works of art and the value of the transaction, or a series of linked transactions, amounts to 10,000 euros or more; or* *(iv) is the operator of a freeport when it, or any other firm or sole practitioner, by way of business stores works of art in the freeport and the value of the works of art so stored for a person, or a series of linked persons, amounts to 10,000 euros or more.'* [ML Regulation 14(1)(d)]
Work of Art	A work of art is as defined in s21(6) to (6B) of the Value Added Tax Act 1994. [See Annex II] [ML Regulation 14(1)(f)]
Term/expression	Meaning
Appropriate person	Someone in a position of responsibility, who knows, and is known by, a customer, and may reasonably confirm the customer's identity. It is not possible to give a definitive list of such persons, but the following may assist AMPs in determining who is appropriate in any particular case: ➢ The Passport Office has published a list of those who may countersign passport applications: see www.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174151
Beneficial owner(s)	The individual who ultimately owns or controls the customer on whose behalf a transaction or activity is being conducted. Special rules have been made for bodies corporate, partnerships, trusts, entities or arrangements that administer and distribute funds and estates of deceased persons. [ML Regulations 5 and 6]
Criminal property	Property which constitutes a person's benefit from criminal conduct or which represents such a benefit (in whole or part and whether directly or indirectly), and the alleged offender knows or suspects that the property constitutes or represents such a benefit. [POCA s 340 (3)]
Criminal conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there.

	[POCA s 340 (2)]
EU Fourth Money Laundering Directive	The Fourth Money Laundering Directive, adopted in 2015 (2015/849EC), updated European Community legislation in line with the revised FATF 40 Recommendations, published in 2012. It was amended by the Fifth Directive.
EC Sanctions Regulation	Regulation 2580/2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
FATF Recommendations	A series of Forty Recommendations on the structural, supervisory and operational procedures that countries should have in place to combat money laundering, issued by the FATF. The Forty Recommendations were originally published in 1990, revised in 1996 and 2004, and last revised in February 2012 and updated in June 2019. FATF issued a series of Special Recommendations on Terrorist Financing in October 2001 and October 2004, and these were subsumed within the revised Forty Recommendations in February 2012. The FATF Forty Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and terrorist financing.
Government-issued	Issued by a central government department or by a local government authority or body.
HM Treasury Sanctions Notices and News Releases	Notices issued by HM Treasury advising firms of additions to the UN Consolidated List maintained under Security Council resolution 1390 (2002) and to the list of persons and entities subject to EC Regulation 2580/2001.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Mind and management	Those individuals who, individually or collectively, exercise practical control over a non-personal entity.
ML Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 [SI 2017/692].
Money laundering	An act which: ➢ constitutes an offence under ss 327, 328 or 329 of POCA or ➢ constitutes an attempt, conspiracy or incitement to commit such an offence or ➢ constitutes aiding, abetting, counselling or procuring the commission of such an offence or

	➢ would constitute an offence specified above if done in the United Kingdom. [POCA, s 340 (11)] A person also commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: ➢ by concealment; ➢ by removal from the jurisdiction; ➢ by transfer to nominees; or ➢ in any other way. [Terrorism Act, s 18]
Nominated officer	A person who is nominated to receive disclosures under Regulation 21(5) and s330 of POCA from others within the firm or organisation who know or suspect that a person is engaged in money laundering. Similar provisions apply under the Terrorism Act.
Occasional transaction	Any transaction which is not carried out as part of a business relationship. [ML Regulation 3 (1)]
Politically exposed person	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, other than as a middle ranking or more junior official. [ML Regulation 35(12)]
Regulated market	A multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is regulated and functions regularly [and in accordance with the provisions of Title III of MiFID]. [MiFID Article 4 1(21)]
Regulated sector	Persons and firms which are subject to the ML Regulations.
Senior management	An officer or employee of a firm in the regulated sector with sufficient knowledge of the firm's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure. [ML Regulation 3]
Senior manager	An individual, other than a director (or equivalent), who is employed by the firm, and to whom the Board (or equivalent) or a member of the Board, has given

	responsibility, either alone or jointly with others, for management and supervision.
Terrorism Act	Terrorism Act 2000, as amended by the Anti-terrorism, Crime and Security Act 2001.
Terrorist property	➢ Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); or ➢ Proceeds of the commission of acts of terrorism; and ➢ Proceeds of acts carried out for the purposes of terrorism "Proceeds of an act" includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). "Resources" includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation. [Terrorism Act, s 14]
Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under POCA ss 337 or 338 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under s 337 or s 338. [POCA, s 333A]
Verification	Verifying the identity of a customer, by reference to documents or information obtained from a reliable source which is independent of the person whose identity is being verified, or of a beneficial owner by taking reasonable measures so that the firm is satisfied that it knows who the beneficial owner is. [Regulation 28(18)] Information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where (a) It is obtained by means of an electronic identification process, including by using electronic means or by using a trust service[5]; and (b) That process is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity. [Regulation 28(19)]

[5] Within the meanings those terms have in Regulation 2014/910/EU of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

1. Risk-based approach

Regulation 18(1),(2),(3)

1.1 Art market participants (referred to in these Guidelines as 'AMPs') are required under the ML Regulations to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which their business is subject, by taking into account:

- information on money laundering and terrorist financing made available by HMRC[6];
- risk factors, including those relating to their customers, countries in which they operate, services they provide, their transactions, services and the delivery channels they use.

Minimum requirements

- Identify and assess the risks of money laundering and terrorist financing to which the business is subject
- Document their risk assessment
- Implement appropriate systems and controls reflecting the degree of risk associated with the business and its customers
- Apply appropriate CDD measures on a risk-sensitive basis, depending for example on the customer, and the nature of the transaction
- Take into account situations which by their nature can present a higher risk of money laundering or terrorist financing, including transactions with PEPs

1.2 To assess the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the AMP, the following steps must be taken

- identify the money laundering and terrorist financing risks that are relevant to the AMP;
- assess the risks presented by the AMP's particular
  - customers (and any underlying beneficial owners);
  - services provided;
  - transactions;
  - delivery channels (for example, private sales, internet platforms);
  - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks, in the context of the nature and size of the AMP's business;
- monitor, review and update the effective operation of these controls; and

[6] https://www.gov.uk/government/collections/hmrc-webinars-email-alerts-and-videos; https://www.gov.uk/topic/business-tax/money-laundering-regulations

- record appropriately what has been done, and why, and the steps taken to communicate the controls within the business.

1.3 Taking a risk-based approach to prevent money laundering and terrorist financing:

- recognises that the money laundering/terrorist financing threat to the AMP varies across customers, jurisdictions, services and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk to their particular business;
- allows senior management to tailor its own approach to the AMP's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

1.4 In considering what steps are appropriate, an AMP must take into account the size and nature of its business. For example, depending on their particular circumstances, AMPs that do not offer high value works of art, do not engage in complex deal structures or have limited or no international exposure would probably have a very simple business risk assessment.

EXAMPLE
An AMP selling contemporary photography with an average value of 5,000 euros (but occasionally over 10,000 euros) from their gallery in Brighton to a south of England customer base would have a very simple risk assessment, compared to an auction house based in London selling paintings with an average value of 50,000 euros or more to an international customer base who frequently transact via agents/proxies.

1.5 The business of many AMPs can be relatively simple, involving few types of artwork, with most customers either being one-off, occasional or known collectors. In such circumstances, a simple approach may be appropriate for most customers, with the focus being on those customers who are assessed to present a higher risk. Other AMPs may see greater volumes of business, but large numbers of their customers may be served through channels (such as online sales platforms, or gallery sales) that offer the possibility of adopting a standardised approach to many AML/CTF procedures. Here, too, the approach for most customers may be relatively straightforward, to reflect the assessed risk.

Regulations 19, 33(7),(8), 37(4),(7)

1.6 Under a risk-based approach, although AMPs start from the premise that most customers are not money launderers or terrorist financiers, they are required to have systems in place (see section 3) to highlight those customers who may indicate that they present a higher risk of this. An AMP uses its assessment of the risks inherent in its business to focus its

risk-based approach on the identification and verification of individual customers.

1.7 No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual AMPs and their customers with a realistic assessment of the threat of the AMP being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact.

1.8 Having a formal AML/CTF policy, and documenting the controls and procedures to implement it, will clarify how the AMP intends to discharge its responsibilities towards the prevention of money laundering and terrorist financing. The policy will also set out how senior management undertakes its assessment of the money laundering and terrorist financing risks the AMP faces, and how these risks are to be managed. Even in the case of a small market participant, a summary of its high-level AML/CTF policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.

Actions required, to be kept under regular review

- Carry out a regular, formal money laundering/terrorist financing risk assessment, including changes in customers and the wider environment
- Ensure internal policies, controls and procedures, including staff awareness, adequately reflect the risk assessment
- Ensure customer due diligence procedures reflect the risk characteristics of customers
- Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers

Business-wide risk assessment

Regulation 18

1.9 Although the ML/TF risks facing an AMP fundamentally arise through its customers, the nature of their businesses and how they transact, an AMP must consider its customer risks in the context of the wider ML/TF environment inherent in the jurisdictions in which it operates.

Regulation 18(2)(b)

1.10 An AMP is required to assess the risks inherent in its business, taking into account risk factors including those relating to its customers, countries or geographical areas in which it operates, its transactions and delivery channels.

Regulation 16(2)

1.11 The UK government has published a national risk assessment of money laundering and terrorist financing[7] which provides the context against

[7] https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017

which an AMP is required to undertake an assessment of the UK risks inherent in its business. AMPs should be aware of this publication, and should take account of relevant findings that affect their individual business risk assessment.

Regulation 18(4),(5),(6)

1.12 Risk assessments must be documented, kept up to date and made available to HMRC on request.

Customer risk assessments

1.13 There is no set format for a customer risk assessment - money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to customers and situations can provide a strategy for managing potential risks by enabling AMPs to subject customers to proportionate controls and monitoring. Typical risk categories include:

- country or geographic risk
- customer risk
- transaction risk.

Country/geographic risk

1.14 Some countries pose an inherently higher money laundering and terrorist financing risk than others. AMPs should check customer location because of the additional risks which arise from cross-border operations. Customers associated with higher risk countries, as a result of their citizenship, country of business or country of residence may present a higher money laundering and terrorist financing risk, taking into account all other relevant factors.

1.15 When identifying the risk associated with countries and geographic areas, AMPs should consider the risk related to:

- the jurisdiction in which the customer (or beneficial owner) is based, or to which they have personal links; and
- the jurisdictions which are the customer´s (or beneficial owner's) main place of business.

1.16 In addition to considering their own experiences, AMPs should take into account a variety of other credible sources of information identifying countries with risk factors in order to determine whether a country and customers from that country pose a higher risk. AMPs may wish to assess information available from FATF and non-governmental organisations which can provide a useful guide to perceptions relating to corruption in the majority of countries.

1.17 The European Commission is empowered to identify high risk third countries with strategic deficiencies in the area of anti-money laundering or countering terrorist financing. The Commission adopted Delegated Regulation 2016/1675 in July 2016. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG.

1.18 Other sources of publicly available information include those from HM Treasury Sanctions[8], FATF high-risk and non-cooperative jurisdictions[9], Moneyval evaluations[10], Transparency International Corruption Perceptions Index[11], FCO Human Rights Report[12], UK Trade and Investment overseas country risk pages[13] and quality of regulation[14].

Customer risk

1.19 The risk posed by an individual customer may be assessed differently depending on whether the customer operates, or is based, in a jurisdiction with a reputation for ML/TF, or in one which has a reputation for strong AML/CTF enforcement.

1.20 Risk factors an AMP may consider when assessing the ML/TF risk posed by customer situations may be grouped under:

- a customer's business or professional activity
- a customer's reputation (or that of a beneficial owner)
- a customer's nature and behaviour
- the way in which the customer approaches the AMP

1.21 Risk factors that may be relevant when considering the risk associated with a customer's (or their beneficial owners') *business or professional activity* include (but are not limited to):

- What is the nature of the customer's business?
- Is the customer from a jurisdiction with low levels of corruption?
- Does the customer or beneficial owner have links to sectors
    - that are associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defence, extractive industries and public procurement?

[8] http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.pdf
[9] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
[10] http://www.coe.int/t/dghl/monitoring/moneyval/
[11] http://cpi.transparency.org/cpi2013/results/
[12] http://www.hrdreport.fco.gov.uk/
[13] http://www.ukti.gov.uk/export/howwehelp/oberseasbusinessrisk/countries.html
[14] http://www.state.gov/eb/rls/othr/ics/2013/index.htm

- that are associated with higher ML or TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?
- that involve significant amounts of cash?

- Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? In what jurisdiction is the PEP, his business or a business he is connected with, located?

- Does the customer or beneficial owner hold another public position that might enable them to abuse public office for private gain?

1.22 The following risk factors may be relevant when considering the risk associated with a *customer's or their beneficial owners' reputation***:**

- Are there any adverse media reports or other relevant information sources about the customer? For example, are there any allegations of criminality or terrorism against the customer or their beneficial owners? If so, are these credible? AMPs should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, among others.

- Is the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?

- Does the AMP have any in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

1.23 The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' *nature and behaviour*:

- Does the customer have legitimate reasons for being unable to provide robust evidence of their identity?

- Does the AMP have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

- Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

- Does the customer request a transaction that is complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose?

- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to disguise the true nature of their business?

- Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments?

1.24 When assessing the risk associated with the *way in which the customer obtains the services*, AMPs should consider a number of factors including:

- Is the customer physically present for identification purposes? If they are not, has the AMP used a reliable form of non-face to face CDD? Has it taken steps to prevent impersonation or identity fraud?

- Has the customer been introduced by a third party, and is the third party regulated for AML? What has the AMP done to be satisfied that:

  i. the third party applies CDD measures and keeps records to UK standards and that it is supervised for compliance with comparable AML/CTF obligations in line with UK requirements?

  ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with UK requirements? and

  iii. the quality of the third party's CDD measures is such that it can be relied upon?

- Has the customer been introduced through an agent? To what extent can the AMP be satisfied that the agent has obtained enough information so that the AMP knows its customer and the level of risk associated with it?

- Where an AMP uses an intermediary, are they:

  i. a regulated person subject to AML obligations that are consistent with those of the UK regime?

  ii. subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/CTF obligations?

  iii. based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high risk third country that the European Commission has identified as having strategic deficiencies, AMPs must not rely on that

intermediary. However, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary undertaking of another AMP established in the EU, and the AMP is confident that the intermediary fully complies with group wide policies, controls and procedures in line with UK requirements.

Transaction risk

1.25 When identifying the risk associated with transactions, AMPs should consider the risk related to

- the level of transparency, or opaqueness;
- the complexity; and
- the value or size of the transaction.

1.26 Risk factors that may be relevant when considering the risk associated with a service or transaction's *transparency* include:

- To what extent does the proposed transaction facilitate or allow anonymity or opaqueness of customer, ownership or beneficiary structures?

- To what extent is it possible for a third party that is not part of the business relationship to give instructions?

1.27 Risk factors that may be relevant when considering the risk associated with a service or transaction's *complexity* include:

- To what extent is the proposed transaction complex and involves multiple parties or multiple jurisdictions?

- To what extent does the proposed transaction involve payments from third parties or accepting overpayments where this is not normally foreseen? Where third party payments are foreseen, does the AMP know the third party's identity? Or is the proposed transaction to be funded exclusively by transfers from the customer's own account at a financial institution that is subject to AML/CTF standards and oversight that are comparable to those required under the UK regime?

1.28 Risk factors that may be relevant when considering the risk associated with a service or *transaction's value or size* include:

- Is the proposed transaction within the AMP's expectations of the customer, given what the AMP knows about his resources and past transactions?

- Is there any cap on transaction values or levels of premium that could limit the attractiveness of the AMP for money laundering or terrorist financing purposes?

Use of risk criteria

1.29 In order to be able to implement a reasonable risk-based approach, AMPs should identify criteria to assess potential money laundering risks. To the extent it is possible, identification of the money laundering or terrorist financing risks presented by customers, or categories of customers, and transactions will allow AMPs to design and implement proportionate measures and controls to mitigate these risks.

1.30 Examples of control procedures include:

- Introducing a customer identification programme (see paragraph 1.33 below) that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing risk;
- Requiring the quality of evidence – whether documentary, electronic or by way of third party assurance - to be of a certain standard;
- Obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing risk; and
- Monitoring customer transactions, where appropriate.

1.31 A customer identification programme that is graduated to reflect risk could involve:

- a standard information dataset and a standard verification requirement for all customers;
- more extensive due diligence (more identification checks and/or requiring additional information) for higher risk customers; and
- where appropriate, more limited identity verification measures for specific lower risk customer/product/transaction combinations.

1.32 Section 5 provides guidance on how customer due diligence obligations might be met.

Risk management is dynamic

1.33 A money laundering/terrorist financing risk assessment is not a one-time exercise. AMPs must therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review.

Regulation 18(4)

1.34 An AMP should therefore keep its risk assessment(s) up to date. It is recommended that the risk assessment is reviewed regularly, probably on an annual basis, and certainly following any significant change in the AMP's business, even if it is decided that there is no case for revision.

1.35 AMPs should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess and, where appropriate, incorporate these in their business-wide and individual risk assessments in a timely manner.

1.36 Examples of systems and controls AMPs could put in place to identify emerging risks include:

- processes to ensure internal information is reviewed regularly to identify trends and emerging issues, both in relation to individual business relationships and to the AMP's business more generally;

- processes to ensure the AMP regularly reviews relevant information sources. This could involve:

  i. regularly reviewing media reports that are relevant to the market sectors or jurisdictions the AMP, and/or its customers, is active in;

  ii. regularly reviewing law enforcement alerts and reports; and

  iii. regularly reviewing thematic reviews and similar publications issued by HMRC.

- engagement with other industry representatives and competent authorities (e.g., at round table meetings, conferences and training) and processes to feed back any findings to relevant staff; and

- establishing a culture of information-sharing within the AMP and strong company ethics.

1.37 Examples of systems and controls AMPs could put in place to ensure their customer and business-wide risk assessments remain up to date include:

- regularly assessing and reviewing their risk assessments, to ensure new or emerging risks are included. Where an AMP is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible; and

- carefully recording issues throughout the year that could have a bearing on the risk assessment, such as internal suspicious transaction reports, compliance failures and intelligence from customer-facing staff, and using this information to update their risk assessment policy.

1.38 Like the original risk assessments, any update of a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate with the ML/TF risk.

2. Nominated officer

Regulation 21 (3) POCA ss337, 338 Terrorism Act ss21A, 21B

2.1 All AMPs (other than sole traders) must appoint a nominated officer[15], who is responsible for receiving disclosures under Part 7 of POCA and Part 3 of the Terrorism Act, deciding whether these should be reported to the NCA, and, if appropriate, making such external reports. The identity of the nominated officer, as well as any subsequent appointment to this position, must be notified to their supervisory authority within 14 days of the appointment. A sole trader with no employees is, by default, the nominated officer.

Regulation 21(8)

2.2 A nominated officer should be able to monitor the day-to-day operation of the AMP's AML/CTF policies, and respond fully and rapidly to enquiries for information made by HMRC or law enforcement. HMRC expect the nominated officer, and any deputy, to be based in the UK.

Minimum requirements

- Nominated officer to be appointed, to oversee AML systems and controls, and, where relevant, receive and review internal disclosures
- Nominated officer is responsible for reporting suspicious activity to the NCA
- Nominated officer should be able to act on his own authority
- Adequate resources must be devoted to AML/CTF

Regulation 19(4)(d) POCA s 330

2.3 Anyone in the AMP to whom information or other matter comes in the course of business as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing is required to make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to them.

2.4 Any internal report must be considered by the nominated officer, in the light of all other relevant information available to the AMP, to determine whether or not the information contained in the report gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

2.5 In most cases, before deciding to make a report, the nominated officer is likely to need access to information on:

- the financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting;
- the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the AMP entered into with or for the customer; and

- the underlying CDD information, and copies of the actual source documentation in respect of the customer.

Regulation 19(4)(d)
Regulation 21(5)
POCA s 331

2.6 If the nominated officer concludes that the internal report gives rise to knowledge or suspicion of money laundering or terrorist financing, he/she must make a report to the NCA as soon as is practicable after he/she makes this determination, even if no transaction takes place. The nominated officer's decision in this regard must be his/her own, and should not be subject to the direction or approval of other parties within the AMP. Failure to report to the NCA is an offence.

2.7 An AMP is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the AMP's AML/CTF policies and procedures, including the operation of the risk-based approach, is primarily the responsibility of the nominated officer, under delegation from senior management. He/she must therefore ensure that appropriate monitoring processes and procedures across the AMP are established and maintained.

Actions required, to be kept under regular review

- Senior management to ensure the nominated officer has:
  - active support of senior management
  - adequate resources
  - independence of action
  - access to information
- Nominated officer to monitor the effectiveness of systems and controls

2.8 Examples of an effective systems and controls arrangement would be one that:

- ensures that policies and procedures reflect current legal and regulatory developments and requirements;
- reflects the adequacy of resources available;
- has appropriate monitoring of outsourced compliance arrangements;
- is supported by adequately trained staff, who are up to date with current developments;
- has appropriate monitoring/quality control/internal review processes;
- provides for appropriate reporting to senior management.

2.9 Where appropriate, senior management should require that the nominated officer provides a regular report covering the operation and effectiveness of the AMP's systems and controls

[15] See https://www.gov.uk/guidance/money-laundering-regulations-nominated-officers-and-employee-training

to combat money laundering and terrorist financing, and should take any action necessary to remedy deficiencies identified by the report in a timely manner.

2.10 The nominated officer will wish to bring to the attention of senior management areas where the operation of AML/CTF controls should be improved, and proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.

2.11 In addition, the nominated officer should report on the outcome of any relevant internal reviews of the AMP's AML/CTF processes, as well as the outcome of any review of the AMP's risk assessment procedures (see paragraph 1.34).

3. Policies, controls and procedures

Regulations 19, 86

3.1 The ML Regulations place an obligation on AMPs to establish adequate and appropriate policies, controls and procedures to mitigate and manage effectively money laundering and terrorist financing risks identified in their risk assessments. The AMP's policies, controls and procedures (and any changes to these), as well as steps taken to communicate these within the business, must be recorded in writing.

Regulation 3(1) 19(2)(b)

3.2 Senior management approval is specifically required for the AMP's policies, controls and procedures for mitigating and managing effectively the risks of money laundering and terrorist financing identified in the AMP's risk assessment.

3.3 For the purposes of the ML Regulations and these guidelines, 'senior management' means officers or employees of the AMP with sufficient knowledge of the AMP's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure. In a single owner/manager business, 'senior management' will be the owner/manager.

Principal actions required

Policies, controls and procedures must require:

- carrying out a risk assessment identifying where the business is vulnerable to money laundering and terrorist financing
- preparing, maintaining and approving a written policy statement, controls and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- reviewing and updating the policies, controls and procedures to reflect changes to the risk faced by the business
- making sure there are enough trained people equipped to implement policies adequately, including systems in place to support them
- making sure that the policies, controls and procedures are communicated within the business, and communicated to and applied to subsidiaries or branches in or outside the UK
- monitoring effectiveness of the business's policy, controls and procedures and make improvements where required
- having systems to identify when transactions are with or through high risk third countries identified by the EU or financial sanctions targets advised by HM Treasury, and taking additional measures to manage and lessen the risk

3.4 The nature and extent of AML/CTF controls will depend on a number of factors, including:

- The nature, scale and complexity of the business
- The geographical diversity of operations
- The customer transaction profile
- The sales channels used, including non face to face access
- The volume and size of transactions
- The extent to which dealing is through intermediaries or third parties

Regulation 19(1)(b), (c), (2)

3.5 An AMP's policies, controls and procedures – which must be documented - must be proportionate with regard to the size and nature of its business, and must be approved by its senior management and kept under regular review.

Regulation 21(10)

3.6 In determining what is appropriate or proportionate with regard to the size and nature of their business, AMPs must take into account their risk assessment and any guidance issued by HMRC or by another appropriate body, and approved by HM Treasury.

Obligations on larger market participants

Regulation 21

3.7 Where appropriate with regard to the size and nature of its business, a larger AMP firm must:

- appoint a member of its board (or equivalent management body) or of its senior management as the officer responsible for the AMP's compliance with the ML Regulations;
- carry out screening of relevant employees appointed by the AMP, both before the appointment is made and during the course of the appointment;
- establish an independent (internal) audit function with the responsibility to:
    - examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by the AMP to comply with the Regulations
    - make recommendations in relation to those policies, controls and procedures
    - monitor the AMP's compliance with those recommendations.

Regulation 21(2)(a)

3.8 Screening of relevant employees (for the purposes referred to in paragraph 3.7 above) means an assessment of:

- the skills, knowledge and expertise of the individual to carry out their functions effectively; and

- the conduct and integrity of the individual.

Regulation 21(2)(b) 3.9 A relevant employee is one whose work is –

- relevant to the AMP's compliance with any requirement in the ML Regulations; or
- otherwise capable of contributing to the
  - identification or mitigation of the risks of ML/TF to which the AMP's business is subject; or
  - prevention or detection of ML/TF in relation to the AMP's business.

Obligations on all market participants

Regulation 19(3) 3.10 The policies, controls and procedures must include:

- risk management practices
- internal controls
- CDD measures and ongoing monitoring, including enhanced measures for high risk customers
- reliance and record keeping
- the monitoring and management of compliance with, and the internal communication of, such policies, controls and procedures.

Regulation 19(4) 3.11 An AMP's policies, controls and procedures must:

- provide for the identification and scrutiny of
  - complex or unusually large transactions, or an unusual pattern of transactions;
  - transactions which have no apparent economic or legal purpose; and
  - any other activity which the AMP regards as particularly likely by its nature to be related to money laundering or terrorist financing.
- specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of transactions which might favour anonymity. This could include putting in place additional due diligence measures;
- assess risk factors relating to delivery channels, including suppliers;
- ensure that when new products, business practices, suppliers or technology are adopted by the AMP, appropriate measures are taken to assess and if necessary mitigate any money laundering or terrorist financing risks that may arise;
- mandate that anyone in the AMP who knows or suspects (or has reasonable grounds for knowing or suspecting) money laundering or terrorist financing must report such knowledge or suspicion to the AMP's nominated officer.

3.12 The AMP's policies, controls and procedures should also cover:

- where appropriate, the arrangements for nominated officer reports to senior management
- the systems for customer identification and verification, including enhanced arrangements for high risk customers, including PEPs
- policy on the use of outsourcing service providers
- the circumstances in which additional information in respect of customers will be sought in the light of their activity
- the procedures for handling SARs, covering both reporting by employees and submission to the NCA
- the mechanisms for contact between the nominated officer and law enforcement or the NCA, including the circumstances in which a defence (that is, appropriate consent) should be sought
- the arrangements for recording information not acted upon by the nominated officer, including reasoning why no further action was taken
- the monitoring and management of compliance with internal policies, procedures and controls
- the communication of such policies, controls and procedures, including details of how compliance is monitored by the nominated officer, and the arrangements for communicating the policies, controls and procedures to all relevant employees;
- employee training records; and
- supporting records in respect of business relationships, and the retention period for the records.

POCA ss 327-330
Terrorism Act s 21A
Regulation 24

3.13 The offences of money laundering under POCA, and the obligation to report knowledge or suspicion of possible money laundering, affect all members of staff of AMPs. The similar offences and obligations under the Terrorism Act also affect all members of staff. However, AMPs have an obligation under the ML Regulations to take appropriate measures to ensure that their employees and agents are made aware of the law relating to money laundering, and terrorist 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 (see section 4).

Regulation 20(1)

3.14 An AMP that is a parent undertaking must ensure that its policies, controls and procedures also apply to all subsidiary undertakings and non-UK branches. Such an AMP must establish and maintain throughout its group, policies, controls and procedures for data protection and sharing, with other members of the group, information for the purposes of preventing money laundering and terrorist financing (including policies on the sharing of information about customers and their transactions) .

Regulation 19(6)

3.15 Where relevant, AMPs must communicate their policies, controls and procedures established to prevent activities related to money laundering

and terrorist financing to branches and subsidiary undertakings located outside the UK.

Regulation 20(3),(4)

3.16 If any subsidiary undertaking or branch is established in a third country which does not impose AML/CTF requirements as strict as those of the UK, the AMP must ensure that such subsidiary undertakings or branches apply measures equivalent to those required by the ML Regulations. Where the law of a non-EEA state does not permit the application of such equivalent measures, the AMP must inform HMRC accordingly, and take additional measures to handle the risk of money laundering and terrorist financing effectively.

Regulation 21(8),(9)

3.17 AMPs must establish and maintain systems which enable them to respond fully and rapidly to enquiries from financial investigators accredited under s3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under the Act or constables, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- the nature of that relationship.

4. Staff training and awareness

Regulation 24(1)

4.1 There are separate obligations on senior management and the business in relation to staff awareness and staff training. The ML Regulations require AMPs to take appropriate measures to ensure that relevant employees and agents are made aware of the law relating to money laundering and terrorist financing (and to data protection, insofar as relevant to the implementation of the ML Regulations), and that they are regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing[16].

Minimum requirements

All AMPs must:

- ensure relevant staff are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation, know who the nominated officer is and what their responsibilities are, trained in the AMP's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
- ensure staff are trained at regular intervals
- maintain a written record of what has been done to raise awareness and the training given to staff
- ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

Larger and more complex AMPs must:

- screen relevant staff before they take up post and during the course of the appointment assess their skill, knowledge and expertise to ensure that they are effective in carrying out their function and are of good conduct and integrity.

Staff training

Regulation 24(1)

4.2 The ML Regulations require AMPs to take appropriate measures so that their relevant employees and agents are:

- made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of the Regulations

[16] See https://www.gov.uk/guidance/money-laundering-regulations-nominated-officers-and-employee-training

- regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.

Regulation 24(1)(b),(3)(a)

4.3 In determining the nature and extent of training measures, AMPs must take account of the nature and size of their businesses, and the nature and extent of the risks of money laundering and terrorist financing to which their businesses is subject.

4.4 AMPs should devise and implement a clear and well-articulated policy and procedure, and maintain a record in writing, for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering and terrorist financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing. AMPs should also monitor the effectiveness of such training, to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.

POCA ss327-329, 334(2)
Terrorism Act ss 18, 21A

4.5 Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. They may also face criminal sanctions if they do not make an internal report to their nominated officer when necessary. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them.

POCA, s 330 (6), (7)
Terrorism Act s21A(5)

4.6 Where a staff member is found to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he/she will have a defence under POCA if he/she has a reasonable excuse for not making the required disclosure. (This is also a defence under the Terrorism Act.)

Regulation 86(1)
Schedule 6, para 5

4.7 A successful defence by a staff member under POCA may leave the AMP open to prosecution or regulatory sanction under the ML Regulations for not having adequate training and awareness arrangements. AMPs should therefore not only obtain acknowledgement from the individual that they have received the necessary training, but should also take steps to assess its effectiveness.

Regulation 24(1)(b)

4.8 AMPs must maintain a record in writing of the appropriate training measures they have taken and, in particular, of the training given to their relevant employees.

4.9 In deciding what training measures are appropriate, an AMP:

- must take account of the nature of its business, its size, and the nature and extent of the money laundering and terrorist financing risks to which its business is subject
- should take account of the guidance issued by HMRC or by another appropriate body and approved by HM Treasury.

4.10 The content of any training, the frequency of training and the assessment of competence following training are matters for each AMP to assess and decide in light of the money laundering and terrorist financing risks they identify, provided the requirements of Regulation 24 are met. HMRC will expect such issues to be covered in each AMP's policies and procedures.

4.11 For example, policies and procedures should make provision for the attainment of an appropriate competence level by the relevant employees identified in paragraph 3.9, prior to them undertaking the duties for which they will be responsible. This may, for example, be achieved by the attainment of an appropriate pass rate in a competency test following training.

4.12 AMPs should also ensure that relevant employees are aware of and understand:

- their responsibilities under the AMP's policies and procedures for the prevention of money laundering and terrorist financing
- the money laundering and terrorist financing risks faced by the AMP
- the AMP's procedures for managing those risks
- the identity, role and responsibilities of the nominated officer, and what should be done in their absence
- the potential effect of a breach upon the AMP and upon its employees
- how the AMP will undertake CDD
- how PEPs, family members of PEPs and known close associates of PEPs will be identified, and how to distinguish PEPs who present a relatively higher risk from those who present a relatively lower risk.

4.13 There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. Online training systems can provide a solution for many employees, but this approach may not be suitable for all employees. Classroom training can be more effective in certain circumstances.

4.14 Procedure manuals, whether paper or electronic, are useful in raising employee awareness and can supplement more dedicated

forms of training, but their main purpose is generally to provide ongoing reference rather than being written as training material.

4.15 Ongoing training must be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness of the training.

4.16 The nominated officer should be involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.

4.17 The NCA publishes a range of material at www.nationalcrimeagency.gov.uk, such as threat assessments and risk profiles, of which AMPs may wish to make their employees aware. The information available on this website could usefully be incorporated into AMPs' training materials. The Home Office publishes guidance that may help staff identify fraudulent identity documents[17]. It is also recommended that AMPs consult HMRC's AML webpage[18], which has useful information (including statements regarding AML controls) and links to other AML resources.

4.18 It is important that the AMP's policies, controls and procedures are communicated widely throughout the AMP, to increase the effectiveness of their implementation.

Actions required

AMPs should ensure that they satisfy the following requirements, and keep the extent to which they are satisfied under regular review:

- provide appropriate training to make relevant staff aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees have information on, and understand, the responsibilities and legal obligations of the business and of members of staff, e.g. the functions of the nominated officer and any changes to these positions
- regularly share risk assessment, policy, control and procedures information within the business
- consider providing relevant staff with case studies and examples related to the AMP's business to illustrate where risks of money laundering and terrorist financing are most likely to arise

[17] Guidance on examining identity documents: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536918/Guidance_on_examining_identity_documents_v._June_2016.pdf

[18] https://www.gov.uk/topic/business-tax/money-laundering-regulations

- train relevant staff in how to operate a risk based approach to assessing the risks of money laundering and terrorist financing and how to accurately verify identity documents
- where appropriate for a larger and/or more complex business set up a system to screen staff before they take up the post and refresh the screening at intervals
- keep records of training given

Staff awareness - alertness to specific situations

4.19 Sufficient training will need to be given to all relevant employees to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing might be taking place.

4.20 The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on the customer and the transaction or service in question. See also paragraphs 1.27-1.30 above.

Example

Illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion, are:

- transactions which make no obvious economic sense (including where a person makes a loss), or which involve apparently unnecessary complexity;
- the use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- where the transaction being requested by the customer is, without reasonable explanation, out of the ordinary range or inconsistent with the experience of the AMP in relation to the particular customer;
- dealing with customers not normally expected in that part of the business;
- transactions involving high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
- unnecessary routing of funds through third party accounts.

4.21 Issues around the customer identification process that may raise concerns include such matters as the following (see also paragraphs 1.21-1.24 above):

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?

- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense?
- Is the staff member aware of any inconsistencies between the information provided and what would be expected, given the location of the customer?
- Is the area of residence given consistent with other known information, such as employment?
- Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the client want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

4.22 Staff should also be on the lookout for such things as:

- transactions made through banks other than those expected;
- large transactions involving countries known for money laundering, terrorism, corruption or drug trafficking;
- significant/unusual/inconsistent participation by third parties in a transaction.

4.23 It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. FATF publishes a regular series of publications on the typologies of financial crime, available at www.fatf-gafi.org.

5. Customer due diligence

Regulation 27(1)

5.1 An AMP must apply CDD measures when it -

(a) establishes a business relationship (see paragraph 5.2);
(b) carries out an occasional transaction (see paragraph 5.3);
(c) suspects money laundering or terrorist financing; or
(d) doubts the veracity of documents or information previously obtained for the purpose of identification or verification.

Regulation 4

5.2 A "business relationship" for CDD purposes is a business, professional or commercial relationship between an AMP (whether a firm or a sole trader) and a customer, involving transactions amounting to 10,000 euros or more, which is connected to the business of the AMP, and is expected by the AMP at the time when contact is established to have an element of duration.

Regulation 3(1), 27(1), (2)

5.3 An "occasional transaction" for CDD purposes means a transaction carried out other than in the course of a business relationship, amounting to 10,000 euros or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. The factors linking 'operations' to assess whether together they constitute a transaction over the 10,000 euros threshold are inherent in the characteristics of the individual transactions – for example, where several payments are received from the same customer, in respect of the same invoice, from one or more sources over a short period of time.

5.4 In the art market, although some AMPs will have a business relationship with some customers, dealing with them regularly, even although at intervals, the majority of transactions are likely to be 'occasional', in that the particular customer makes a one-off purchase or sale and there is no certainty of repeat custom.

Who is the 'customer' for CDD purposes?

Regulation 28(2)

5.5 The "customer" for the purposes of the ML Regulations will vary, depending on the AMP's business model. It will be the purchaser of a work of art, and any broker or agent acting for them. It will be the seller, where the AMP provides a service to, and receives financial value from, them.

5.6 The AMP conducting the transaction must apply CDD measures to the customer, so that they can identify the customer and, where necessary, the source of funds.

5.7 This is in addition to an AMP's continuing obligations under POCA (and additional obligations because the AMP is now in the regulated sector – see paragraphs 6.15, 6.18 and 6.34 below) to ensure that they neither know or suspect, nor have reasonable grounds for knowing or

suspecting, that they are handling or facilitating a sale of a work of art which itself represents the proceeds of crime. They also have obligations under UK and EU sanction regimes to ensure that they are not dealing or transacting with any sanctioned person. To meet POCA and sanctions obligations, therefore, it may be appropriate (as determined on a risk-based approach) for an AMP to carry out further checks on the seller or consignor of a work of art, to ensure that they are not handling stolen works of art, or otherwise facilitating use of the proceeds of crime.

5.8 Where a customer is acting as an agent, the AMP conducting the transaction has an obligation under the ML Regulations to carry out CDD on the agent and also on the ultimate customer, as an AMP must know the identity of the person who is ultimately paying for the work of art. The AMP must also verify that the agent is authorised to act on behalf of the customer. An AMP acting as a selling agent has an obligation to carry out CDD on the person on whose behalf they are selling the artwork. The buyer, or his agent, however, has no obligation or right to know the identity of the ultimate seller.

Regulation 6(9)

5.9 A beneficial owner is usually an individual who ultimately owns or controls a customer who is body corporate or a partnership, or on whose behalf a transaction is being conducted.

Regulation 5(1), (2), (3)

5.10 The ML Regulations define beneficial owners as individuals either ultimately owning or controlling more than 25% of body corporates or partnerships or otherwise owning or controlling the customer. These individuals must be identified, and reasonable measures must be taken to verify their identities.

5.11 There is no requirement on AMPs to make proactive searches for beneficial owners in respect of private individuals (who might be assumed to be buying for themselves), unless it appears that the customer is not acting on his own behalf.

Persons and entities subject to financial sanctions

5.12 The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions, in accordance with relevant legislation. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target.

5.13 A Consolidated List of all targets to whom financial sanctions apply is maintained by the Office of Financial Sanctions Implementation (OFSI), and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at: www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

5.14 The obligations under the UK financial sanctions regime apply to AMPs (and not just to banks). The Consolidated List includes all the names of designated persons under UN, EC and UK sanctions regimes which have effect in the UK. AMPs will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although an AMP doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. Other websites may contain useful background information, but the purpose of the HM Treasury list is to draw together in one place all the names of designated persons for the various sanctions regimes effective in the UK. All AMPs to whom this guidance applies, therefore, whether or not they are registered with HMRC, will need either:

- for manual checking: to register with the HM Treasury update service (directly or via a third party, such as a trade association); or
- if checking is automated: to ensure that relevant software includes checks against the relevant list and that this list is up to date.

5.15 OFSI may also be contacted direct to provide guidance and to assist with any concerns regarding the implementation of financial sanctions:

Office of Financial Sanctions Implementation
HM Treasury
1 Horse Guards Road
LONDON SW1A 2HQ
Tel: +44 (0) 20 7270 5454
Email: ofsi@hmtreasury.gsi.gov.uk

5.16 AMPs need to have some means of monitoring payment instructions to ensure that proposed payments to sanctioned individuals or entities or to their agents are not made.

5.17 Where an AMP has suspicions of terrorist financing, it must make a report to OFSI, and/or to the NCA. Guidance on such reporting is given in paragraphs 6.18-6.26.

5.18 Trade sanctions can be imposed by governments or other international authorities, and these can have implications for the art market. Where the proposed trade deal also involves a person or entity which is subject to an asset freeze, an AMP will need a licence from OFSI to deal with the funds of the designated individual, as well as, potentially, an export licence from the Department for International Trade. AMPs which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the AMP's procedures. Further information and links to lists of affected countries can be found at: https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions.

5.19 The following tables set out the obligations of the various parties involved:

A. Private sales or purchases	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Regulated Dealer/Gallery is **selling** a work of art to a Buyer.	Dealer/Gallery		Yes, buyer is a customer
Regulated Dealer/Gallery is **selling** a work of art to a Buyer, on behalf of a Seller.	Dealer/Gallery	Yes, the Seller is a customer.	Yes, Buyer is a customer
Regulated Dealer/Gallery is **selling** a work of art to a Buyer. An Agent is acting for the Buyer *but the Buyer is paying the regulated dealer/gallery direct*.	Dealer/Gallery		Yes, Buyer and their Agent are both customers.
Regulated Dealer/Gallery is **selling** a work of art to a Buying Dealer. The Buying Dealer has confirmed that they are buying with their own money.	Dealer/Gallery		Yes, Buying Dealer is the customer.
	Buying Dealer, if regulated	Dealer/Gallery is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	

A. Private sales or purchases	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Regulated Dealer/Gallery is **selling** a work of art to a Buying Dealer. The Buying Dealer has confirmed that they are acting for an underlying Buyer *who will put the Buying Dealer in funds to pay for the work of art*.	Dealer/Gallery		Yes, for the Dealer/Gallery the Buyer and the Buying Dealer are both customers.
	Buying Dealer, if regulated	Dealer/Gallery is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	Yes, for the Buying Dealer if regulated, the Buyer is the customer.
Regulated Dealer/Gallery is **selling** a work of art to a Buying Dealer. The Buying Dealer has said that they are buying with their own money, but the Dealer/Gallery suspects they are paying with money from an underlying client.	Dealer/Gallery		Yes, Buying Dealer is the customer. Dealer/ Gallery should consider whether "enhanced due diligence" is appropriate, in view of suspicions over source of funds. If funds are coming from an underlying Buyer, they are also a customer.
	Buying Dealer, if regulated	Dealer/Gallery is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	

A. Private sales or purchases	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Regulated Dealer/Gallery is **buying** a work of art from a Seller.	Dealer/Gallery	Seller is not a customer of Dealer/Gallery for CDD purposes see paragraph 5.5), but the Dealer/Gallery still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	
Regulated Dealer/Gallery is **buying** a work of art from a Seller who is represented by an Agent. *Payment will transfer direct to the Seller*.	Dealer/Gallery	Neither Seller nor Agent are customers of Dealer/Gallery for CDD purposes see paragraph 5.5), but the Dealer/Gallery still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	
	Agent, if regulated	Yes, Seller is a customer of the Agent.	

B. Auction sales	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Seller is consigning a work of art to a Regulated Auction House for sale.	Auction House	Yes, Seller is a customer.	
Regulated Auction House is selling a work of art at auction to a Buyer.	Auction House	Yes, Seller is a customer.	Yes, Buyer is a customer
Regulated Auction House is selling a work of art to a Buyer. An Agent will bid for the Buyer *but the Buyer is paying direct*.	Auction House	Yes, Seller is a customer.	Yes, Buyer and Agent are customers.

B. Auction sales	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Regulated Auction House is selling a work of art to a Dealer. The Dealer has confirmed that they are buying with their own money.	Auction House	Yes, Seller is a customer.	Yes, the Dealer, as buyer, is the customer.
	Regulated Dealer	The Auction House is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	
Regulated Auction House is selling a work of art to a Dealer. The Dealer has confirmed that they are acting for an underlying Buyer *who will put the Dealer in funds to pay for the work of art*.	Auction House	Yes, Seller is a customer.	Yes, the Dealer *and* the Buyer are customers.
	If regulated, the Dealer acting for the Buyer	The Auction House is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	Yes, for the Dealer if Regulated, the Buyer is the customer.

B. Auction sales	Who must conduct CDD checks	CDD on Seller?	CDD on Buyer?
Regulated Auction House is selling a work of art to a Buying Dealer. The Buying Dealer has said that they are buying with their own money, but the Auction House suspects they are paying with money from an underlying client.	Auction House	Yes, Seller is a customer.	Yes, Buying Dealer is the customer. Auction House should consider whether "enhanced due diligence" is appropriate, in view of suspicions over source of funds. If funds are coming from an underlying Buyer, they are also a customer.
	Buying Dealer, if regulated	The Auction House is not a customer of Buying Dealer for CDD purposes (see paragraph 5.5), but the Buying Dealer still has POCA/sanctions obligations (see paragraph 5.7 and 5.8).	

Applying CDD measures

Regulation 30(2)

5.20 The verification of the identity of the customer and, where applicable, the beneficial owner, must take place before establishing a business relationship or concluding a transaction. In practice, this means before release of the art work to the customer.

Minimum requirements

AMPs must:

- complete customer due diligence on all customers and beneficial owners before concluding a transaction that requires due diligence
- identify and verify a person acting on behalf of a customer and verify that they have authority to act
- apply enhanced due diligence to take account of the greater potential for money laundering or terrorist financing in higher risk cases, including in respect of PEPs, and customers established in high-risk third countries

- not deal, or cease a transaction, with certain persons or entities if they cannot carry out customer due diligence and consider making a suspicious activity report
- have a system for keeping copies of customer due diligence and supporting records and keep the information up to date.

Regulation 28(1)

5.21 Applying CDD measures involves several steps. The AMP is required to *identify* customers (and, where applicable, that of beneficial owners) and then to *verify* their identity and assess the purpose and intended nature of the business relationship or occasional transaction.

5.22 An AMP trading, or arranging the trade of, a work of art has an obligation to carry out CDD on the customer and on any agent or ultimate beneficial owner of the customer.

Regulation 28(12)

5.23 Based on the risk assessment carried out (as described in section 1), an AMP will, based on their risk assessment, determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customers, based on the AMP's risk appetite.

Regulation 28(2)(c)

5.24 An AMP must also understand the purpose and intended nature of the proposed transaction to assess whether it is in line with the AMP's expectation of the customer. In most instances this will be self-evident, but in many cases the AMP may have to obtain information in this regard.

5.25 Depending on the AMP's risk assessment of the situation, information that might be relevant may include some or all of the following:

- nature and details of the business/occupation/employment;
- the expected source and origin of the funds to be used in the transaction;
- the origin of the customer's source(s) of wealth and funds;
- the various relationships between signatories and with any underlying beneficial owners.

Regulation 39(7)(8)

5.26 Nothing in the ML Regulations prevents an AMP applying CDD measures by means of an agent or an outsourcing service provider, provided that the arrangements between the AMP and the agent or outsourcing service provider provide for the AMP to remain liable for any failure to apply such measures.

5.27 Documents or information obtained for the purposes of applying CDD measures, held about customers with whom the AMP has a business relationship, must be monitored, to ensure it is kept up to date. Once the identity of such a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); as risk dictates, however, AMPs must take

steps to ensure that they hold appropriate up-to-date information on their customers.

5.28 Although keeping customer information up-to-date is required under the ML Regulations, this is also a requirement of the Data Protection Act in respect of personal data.

Regulation 31(1)

5.29 However, if an AMP cannot:

- satisfy itself as to the identity of a customer or the beneficial owner or controller of the customer;
- verify that identity;
- obtain sufficient information on the nature and intended purpose of the relationship; or
- has doubts over the veracity or adequacy of documents or information previously obtained for the purposes of identification,

the ML Regulations require that it must not conclude the transaction, and consider making a disclosure under POCA or the Terrorism Act.

Evidence of identity

Regulation 28(2)(a)(b),(18)

5.30 The AMP *identifies* a customer by obtaining a range of information about him. A customer's identity must then be *verified* on the basis of documents or information obtained from a reliable source which is independent of the customer. It is therefore important that the evidence used to verify identity meet this test.

5.31 Evidence of identity can be obtained in a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photocard driving licences, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation, including, in appropriate circumstances, written assurances from persons or organisations, independent of the customer, that have dealt with the customer for some time.

5.32 Part of the AMP's control framework will involve decisions as to whether verification should take place electronically, and the extent to which the AMP can use customer verification procedures carried out by other AMPs. AMPs must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, or transaction.

5.33 A person's identity can be verified in different ways, for example by:

- obtaining or viewing original documents and ensuring that they are valid and genuine, by comparing them to published, authoritative guidance that outlines security features (which protect against forgeries)
- comparing the likeness of the person to the document (for example, photograph comparison or comparison of information)
- conducting electronic verification through a scheme which properly establishes the customer's identity, not just that the customer exists
- obtaining information from another person in the regulated sector (for example, from a bank), that can be used in conjunction with other documents and information to prove a customer's legitimacy over time, or to provide other positive or negative information.

5.34 An increasing amount of data on individuals is held electronically/digitally, in various forms, and by various organisations. Like documents, sources of electronic information about individuals can, of course, vary in integrity and in reliability and independence in terms of their technology and content. Electronic databases, however, are becoming ever more sophisticated and widespread, and are likely to be increasingly used; AMPs should be satisfied that their choice of such sources meets the CDD test of reliability and independence.

Regulation 28(12)

5.35 How much identity information or evidence to ask for, the balance between asking for documents and using electronic sources, and what to verify, in order to be reasonably satisfied as to a customer's identity, and to guard against impersonation, are matters of judgement, which must be exercised on a risk-based approach, taking into account factors such as:

- the nature of the transaction sought by the customer;
- the nature and length of any existing or previous relationship between the customer and the AMP;
- the nature and extent of any assurances from other regulated AMPs that may be relied on; and
- whether the customer is physically present.

An appropriate record of the steps taken, and copies of, or references to, the evidence obtained to identify the customer must be kept.

Documentary evidence

5.36 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, with no, or only very limited, checks being carried out.

Clearly, the level of risk determined to be presented by a customer will determine the verification level that should be required lies on this spectrum. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by other regulated firms, including those in the financial services sector; then
- those issued by other AMPs subject to the ML Regulations, then
- those issued by other organisations.

5.37 In their procedures, therefore, AMPs will in many situations need to be prepared to accept a range of documents, assessing the appropriateness of each according to the risk presented by the customer.

5.38 AMPs should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, AMPs should take whatever practical and proportionate steps are available to establish whether the document offered has been reported as lost or stolen.

Electronic evidence

5.39 AMPs may choose to use electronic/digital identity checks where this is possible, either on their own or in conjunction with documentary evidence.

5.40 Some electronic sources evidencing identity can be created by commercial organisations from a range of other existing electronic material, without any requirement that the source meet particular verifiable performance or other standards in doing so. Others may be established against specific transparent criteria, and be subject to independent verification and assessment of their processes against these criteria, both initially and on an ongoing basis. AMPs should understand the basis upon which any particular source is established and whether, and if so how, its compliance with specific criteria, and performance are monitored.

5.41 Electronic data sources can provide a wide range of confirmatory material without directly involving the customer, although the customer's permission may be required for the AMP to have access to a particular source. Some sources focus on using primary identity documents, sometimes using biometric data. Others accumulate corroborative information which in principle is separately available elsewhere. Some sources are independent of the customer, whilst others are under their 'control' in the sense that their approval is required for information to be included.

5.42 In using an electronic or digital source to verify a customer's identity, AMPs should ensure that they are able to demonstrate that they have both verified that the customer (or beneficial owner or agent) exists, and satisfied themselves that the individual or entity seeking the

business relationship or transaction is, in fact, that customer (or beneficial owner). The use of biometric information is one way of achieving the latter confirmation, as is the use of private information or codes that incontrovertibly link the potential customer (or beneficial owner) to the electronic/digital identity information.

5.43 AMPs should recognise that some electronic sources may be more easily tampered with, in the sense of their data being able to be amended informally and unofficially, than others. If suspicions are raised in relation to the integrity of any electronic information obtained, AMPs should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant source should be used.

Nature of electronic checks

5.44 A number of commercial organisations which access many data sources are accessible online by AMPs, and may provide a composite and comprehensive level of electronic verification through a single interface. Such organisations use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a PEP or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

5.45 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Some electronic sources or digital identity schemes specify criteria-driven levels of authentication that are established through the accumulation of specific pieces of identity information.

5.46 Such information should include data from more robust sources - where an individual has had to prove their identity, or address, in some way The information maintained should be kept up to date, and the organisation's verification – or re-verification - of different aspects of it should not be older than an agreed period, set by the AMP under its risk-based approach.

5.47 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

5.48 For an electronic/digital check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register), or at a single point in time, is not normally enough on its own to verify identity.

Criteria for use of a provider of electronic verification of identity

5.49 Some commercial organisations providing electronic/digital verification are free-standing and set their own operating criteria, whilst others may be part of an association or arrangement where organisations can become accredited by requiring them to demonstrate that they meet certain published criteria – for example, in relation to data sources used, or how current their information is - and carry out checks on continuing compliance.

5.50 Before using a commercial organisation for electronic verification of identity, AMPs should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate, and independent of the customer. This judgement may be assisted by considering whether the identity provider meets the following criteria:

- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
- unless it is on the Information Commissioner's list of credit reference agencies (see https://ico.org.uk/for-the-public/credit/), it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards;
- it uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources;
- its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;
- arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed; and
- it has transparent processes that enable the AMP to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

5.51 In addition, a commercial organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity.

Standard customer due diligence

5.52 A customer's identity for the purposes of CDD consists of a number of aspects, including the customer's name, current and past addresses, date of birth, place of birth,

physical appearance, employment and financial history, and family circumstances.

5.53 The identity of a customer who is not a private individual consists of a combination of its constitution, its business, its legal form and its ownership and control structure.

Private individuals

5.54 For the two steps of *identification* and *verification*, paragraphs 5.55 to 5.74 refer to the standard evidence requirement for customers who are private individuals; paragraphs 5.75 to 5.77 provide further guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

Identification

5.55 The AMP should obtain the following information in relation to the private individual:

- full name
- residential address
- date of birth

Verification

Regulation 28(18) 5.56 Verification of the information obtained must be based on reliable sources, independent of the customer – which might either be a a document, or electronically by the AMP, or by a combination of both. Documents issued or made available by an official body are regarded as independent of the customer, even if they are provided or made available to the AMP by the customer. Where business is conducted face-to-face, AMPs should, where reasonable and appropriate, ask to see originals of any documents involved in the verification. Customers should be discouraged from sending original valuable documents by post.

Documentary evidence

5.57 If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court or local authority, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the AMP reasonable confidence in the customer's identity, although the AMP should weigh these against the risks involved.

5.58 Non-government-issued documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another regulated firm, whether an AMP or a financial services firm, or is supplemented by documented knowledge that the AMP already has of the person or entity, which it has documented.

5.59 If identity is to be verified from documents, this should be based on :

Either a government-issued document which incorporates:

- the customer's full name and photograph, and
    - **either** his residential address
    - **or** his date of birth.

Government-issued documents with a photograph include:

- Valid passport
- Valid photocard driving licence (full or provisional)
- National Identity card
- Firearms certificate or shotgun licence
- Identity card issued by the Electoral Office for Northern Ireland

or a government, court or local authority-issued document (without a photograph) which incorporates the customer's full name, ***supported by*** a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another regulated AMP, which incorporates:

- the customer's full name and
    - **either** his residential address
    - **or** his date of birth

Government-issued documents without a photograph include:

- Valid (old style) full UK driving licence
- Instrument of a court appointment (such as liquidator, or grant of probate)
- Current council tax demand letter, or statement

5.60 Examples of other documents to support a customer's identity include current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK or EU, or utility bills. If the document is from the internet, a pdf version may be more reliable (but see paragraph 5.43). Where a member of the AMP's staff has visited the customer at his home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (i.e., equivalent to a second document).

5.61 In practical terms, this means that, for face-to-face verification, production of a valid passport or photocard driving licence (so long as the photograph is in date[19]) should enable most individuals to meet the identification requirement for AML/CTF purposes**.** The AMP's risk-based procedures may dictate additional checks for the management of credit and fraud risk, or may restrict the use of certain options, e.g., restricting the acceptability of National Identity Cards in face-to-face business in the UK to cards issued only by EEA member states and Switzerland.

5.62 Some consideration should be given as to whether the documents relied upon are, or appear to be, forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity. Commercial software is also available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

Electronic evidence

5.63 When using an electronic/digital source to verify a customer's identity, AMPs should ensure that they are able to demonstrate that they have both verified that the customer exists, and satisfied themselves that the individual seeking the business relationship or transaction is, in fact, that customer (or beneficial owner or agent).

5.64 Electronic verification may be carried out by the AMP either direct, using as its starting point the customer's full name, address and date of birth, or through an organisation which meets the criteria in paragraphs 5.49 and 5.50.

5.65 For verification purposes, an AMP may approach an electronic/digital source of its own choosing, or the potential customer may elect to offer the AMP access to an electronic/digital source that he/she has already registered with, and which has already accumulated verified evidence of identity, and which meets the criteria in paragraphs 5.49 and 5.50.

5.66 Some electronic sources focus on using primary identity documents, sometimes using biometric data. Others accumulate corroborative information which in principle is separately available elsewhere. Some sources are independent of the customer, whilst others are under their 'control' in the sense that their approval is required for information to be included.

5.67 As well as requiring a commercial organisation used for electronic verification to meet the criteria set out in paragraphs 5.49 and 5.50, it is important that the process of electronic verification meets an appropriate level of confirmation before it can be judged to satisfy the AMP's legal obligation.

[19] It should be noted that as well as a general expiry date for UK driving licences, the photograph has a separate expiry date (10 years from first issue). Northern Ireland driving licences have a single expiry date, which is ten years from date of issue.

5.68 Commercial organisations that provide electronic verification of identity use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Some organisations confirm that a given, predetermined 'level' of authentication has been reached. AMPs should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.44 to 5.48, and cumulatively meet an appropriate level of confirmation in relation to the risk assessed in the relationship.

Mitigation of impersonation risk

5.69 Whilst some types of transaction have traditionally been conducted on a non-face-to-face basis, transactions and relationships are now increasingly undertaken in this way: e.g., over the internet and by telephone.

5.70 Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non face-to-face business, there are other factors that may, taken together, aggravate the typical risks:

- the ease of access to the facility, regardless of time and location;
- the ease of making multiple fictitious approaches without incurring extra cost or the risk of detection;
- the absence of physical documents; and
- the speed of electronic transactions.

5.71 The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the service provided and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is often not physically present - such as in online auctions - which would not in itself increase the risk attaching to the transaction. An AMP should take account of such cases in developing their systems and procedures, including consideration of whether the risk is raised to the point that EDD is required.

5.72 Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.

5.73 Where identity is verified electronically, copy documents are used, or the customer is not physically present, an AMP should apply an additional verification check to manage the risk of impersonation fraud. In this regard, AMPs should consider:

- verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or

- requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs or other secret data may be set up within the electronic/digital identity,

or may be supplied to a verified mobile phone, on a one-time basis, or

- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of relevant documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration); or

- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; or

- requiring copy documents to be certified by an appropriate person

5.74 The source(s) of information used to verify that an individual exists may be different from those sources used to verify that the potential customer is in fact that individual.

Other considerations

5.75 The standard identification requirement (for documentary or electronic approaches) is likely to be sufficient for most situations. If, however, the customer, and/or the transaction, is assessed to present a higher money laundering or terrorist financing risk – for example, because of the nature of the customer, or his business, or its location, or because of proposed features of the transaction – EDD is required, and the AMP will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

5.76 Where the result of the standard verification check gives rise to concern or uncertainty over identity, or other risk considerations apply, so the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase.

5.77 For higher risk customers with whom the AMP has a business relationship, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see paragraphs 5.156ff and 5.213/214).

Executors and personal representatives

Regulation 6(6)

5.78 In the case of an estate of a deceased person in the course of administration, the beneficial owner is

- in England and Wales and Northern Ireland, the executor, original or by representation, or administrator for the time being of a deceased person; and
- in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900[20].
-

5.79 In circumstances where a transaction is proposed by executors or administrators for the purpose of winding up the estate of a deceased person, AMPs may accept the court documents granting probate or letters of administration as evidence of authority of those personal representatives. Lawyers and accountants acting in the course of their business as regulated firms, who are not named as executors/administrators, can be verified by reference to their practising certificates, or to an appropriate professional register.

Attorneys

5.80 When a person enters into a transaction under a power of attorney, that person is also a customer of the AMP. Consequently, the identity of holders of powers of attorney should be verified, in addition to that of the donor.

5.81 Other than where the donor or grantor of a power of attorney is an existing customer of the AMP, his identity must be verified. In some cases, these customers may not possess the standard identity documents referred to in paragraphs 5.57ff, and AMPs may have to accept alternative documentation. There may also be cases where the donor or granter is not able to perform face-to-face identification (e.g., disabled, home bound, remote location); due consideration should be given to the individual's circumstances in such cases.

5.82 New Enduring Powers of Attorney are no longer able to be entered into, but where one has already been registered with the Office of the Public Guardian, the AMP will know that the donor has lost, or is losing, capacity. A Lasting Power of Attorney cannot be used until it has been registered, but, subject to any restrictions, this may be done at any time, including while the donor is still able to manage their affairs. Therefore, the AMP will not necessarily know whether or not the donor has lost capacity.

Other AMPs that are subject to the ML Regulations (or equivalent)

5.83 Customers which are subject to the ML Regulations or equivalent, but which are not regulated in the UK, the EU or an assessed low risk jurisdiction, should be treated, for AML/CTF purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in paragraphs 5.108 to 5.114; or if partnerships, by confirming their regulated status through reference to the current membership directory of the relevant professional association (for example, law society or accountancy body). However, when professional individuals are acting in their personal capacity, for

[20] 1900 c.55. Sections 6 and 7 were amended by the Succession (Scotland) Act 1964 (c.41)

example, as trustees, their identity should normally be verified as for any other private individual.

5.84 AMPs should take appropriate steps to be reasonably satisfied that the person the AMP is dealing with is properly authorised by the customer.

5.85 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Corporate customers (other than regulated firms)

5.86 The identity of a customer who is not a private individual consists of a combination of its constitution, its business, its legal form and its ownership and control structure.

5.87 Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, AMPs should take account of the availability of public information in respect of different types of company.

Regulation 43

5.88 Most UK body corporates have obligations to maintain up-to-date information on people with significant influence and control over them and file this information at Companies House. This is known as the central register of people with significant control (PSC register), and is accessible online without charge. When a UK body corporate enters into a business relationship with an AMP, where the AMP is required to apply CDD measures, the corporate must on request provide the AMP with:

- information identifying
  - its name, registered number and principal place of business;
  - its board of directors
  - its senior management
  - the law to which it is subject
  - its legal and beneficial owners;
- its articles of association or other governing documents.

Guidance on the requirements to maintain PSC registers is available at https://www.gov.uk/government/publications/guidance-to-the-people-with-significant-control-requirements-for-companies-and-limited-liability-partnerships.

Regulation 28(3)(b)

5.89 An AMP must take reasonable measures to determine and verify the law to which the corporate is subject, and its constitution (whether set out in its articles of association or other governing document).

Regulation 30A

5.90 In reporting discrepancies discovered in company registers, AMPs should have regard to guidance issued by Companies House[21].

5.91 The structure, ownership, purpose and activities of the great majority of corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering or terrorist financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering or terrorist financing.

Regulation 28(4)(c)

5.92 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. AMPs should make an evaluation of the effective distribution of control in each case. What constitutes control for this purpose will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

Regulation 28(3)(a), (3A)

5.93 As well as obtaining the information set out in paragraph 5.97, to the extent consistent with the risk assessment carried out in accordance with the guidance in section 1 the AMP must take reasonable measures to understand the company's legal form and ownership and control structure, and must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking to enter into the transaction.

Regulation 5(1)

5.94 In the case of a body corporate, other than a company listed on a regulated market, the beneficial owner includes any individual who:

- ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings or by other means) more than 25% of the shares or voting rights in the body corporate; or
- exercises control over the management of the body corporate; or
- otherwise exercises significant influence or control over the body corporate.

For example, if no individual owns or controls more than 25% of the shares or voting rights in the body, AMPs should use judgement in determining whether an individual owning or controlling a lower percentage exercises effective control. Guidance on the meaning of other forms of significant influence and control is available for companies:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621687/psc-statutory-guidance-companies.pdf

[21] https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity

Limited Liability Partnerships: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/523122/Draft_statutory_guidance_LLPs.pdf ; and Eligible Scottish Partnerships: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621569/170622_Eligible_Scot_P_GUI_June_2017.pdf

5.95 Directors of a body corporate do not fall under the definition of beneficial owner in their capacity of director. However, a director may as an individual or legal person also hold an ownership interest in the body, or fall into one of the other categories of exercising significant influence or control over the body.

5.96 Paragraphs 5.97 – 5.114 refer to the standard evidence for corporate customers, and paragraphs 5.115 – 5.118 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

Regulation 28(3)(a)

5.97 The AMP must obtain and verify the following information in relation to the corporate concerned:

- full name
- registered number
- registered office address in country of incorporation
- principal business address (if different from the registered office)

and, additionally, for private or unlisted companies:

- names of individuals who own or control over 25% of its shares or voting rights
- names of any individual(s) who otherwise exercise control over the management of the company

Regulation 28(3) (3A)

5.98 The AMP must take reasonable steps to determine and verify:

(a) the law to which the corporate is subject;
(b) its constitution (whether set out in its articles of association or other governing documents);
(c) names of its directors and the senior persons responsible for its operations.

The AMP must take reasonable measures to understand the company's legal form and ownership and control structure, and should verify the information set out in paragraph 5.97, and in (a)-(c) above, from appropriate sources, such as:

- confirmation of the company's listing on a regulated market
- a search of the relevant company registry
- a copy of the company's Certificate of Incorporation

5.99 AMPs must take appropriate steps to be reasonably satisfied that the person the AMP is dealing with is properly authorised by the customer.

5.100 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Companies listed on regulated markets (EEA or equivalent)

5.101 Corporate customers whose securities are admitted to trading on a regulated market in an EEA state or one in an assessed low risk jurisdiction are publicly owned and generally accountable.

Regulation 28(5)

5.102 Where the AMP has satisfied itself that the customer is:

- a company which is listed on a regulated market (within the meaning of MiFID) in the EEA, or on a non-EEA market that is subject to specified disclosure obligations; or
- a majority-owned and consolidated subsidiary of such a listed company

the obligation to identify, and to verify the identity of, beneficial owners, and the obligation to take reasonable steps to determine and verify the information at 5.98 (a)-(c) does not apply (see paragraphs 5.186ff). Thus, simplified CDD may be applied.

Regulation 3(1)

5.103 Specified disclosure obligations are disclosure requirements consistent with specified articles of:

- The Prospectus directive [2003/71/EC]
- The Transparency Obligations directive [2004/109/EC]
- The Market Abuse Regulation[2014/596]

and with EU legislation made under these specified articles.

Regulations 3(1) and 37(3)(a)(iv)

5.104 If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. AMPs should, however, record the steps they have taken to ascertain the status of the market. If the market is outside the EEA, but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligation in the EU, similar treatment is permitted. For companies listed outside the EEA on markets which do not meet the requirements set out in paragraph 5.103, the standard verification requirement for private and unlisted companies should be applied.

5.105 ESMA maintains a list of regulated markets within the EU at https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_mifid_rma

Other publicly listed or quoted companies

5.106 Companies that are listed on a regulated market that is not equivalent and thus where in principle an obligation to verify beneficial owners remains, are still subject to some degree of accountability and transparency. As part of their risk-based approach, therefore, AMPs may have regard to 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 required and the extent to which the customer should be treated as a private company (see paragraphs 5.108 - 5.114).

5.107 In applying the risk based approach, AMPs may take into account the potentially lower risk presented by companies whose shares are traded as this makes them less likely to be established for money laundering purposes. However, the AMP should, for markets that allow listed companies to have dominant shareholders (especially where they are also directors), ensure that such cases are examined more closely.

Private and unlisted companies

5.108 Unlike publicly quoted companies, the activities of private or unlisted companies are often carried out for the profit/benefit of a small and defined group of individuals or entities. Such companies are also subject to a lower level of public disclosure than public companies. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable. Information from the central PSC register will also be available.

Regulation 33(1)(g)

5.109 Where private companies are well known, reputable organisations, with long histories in their industries and substantial public information about them, the standard evidence may well be sufficient to meet the AMP's obligations. Where a higher risk of money laundering is associated with the business relationship, however, EDD must be applied.

5.110 In the UK, a company registry search will confirm that the applicant company has not been, or is not in the process of being, dissolved, struck off or wound up. In the case of non-UK companies, AMPs should make similar search enquiries of the registry in the country of incorporation of the applicant for business.

5.111 Standards of control over the issue of documentation from company registries vary between different countries. Attention should be paid to the jurisdiction the documents originate from and the background against which they are produced.

5.112 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, AMPs should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may

influence its operations (political connections, etc). Where appropriate, a visit to the place of business may be helpful to confirm the existence and activities of the entity.

Directors

5.113 An AMP will have identified all the directors of a corporate customer (see paragraph 5.97 above). Following the AMP's assessment of the money laundering or terrorist financing risk presented by the company, it has to decide, as appropriate, which directors' identities should be verified in accordance with the guidance for private individuals (paragraphs 5.55 to 5.74). Verification is likely to be appropriate for those who have authority to give the AMP instructions concerning the use or transfer of funds, but might be waived for other directors. AMPs may, of course, already be required to verify the identity of a particular director as a beneficial owner if the director owns or controls more than 25% of the company's shares or voting rights (see paragraph 5.94).

Beneficial owners

Regulation 5
Regulation 28(4),(7),(9)

5.114 (a) As part of the standard evidence, the AMP should know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. The AMP must take reasonable measures to verify the identity of those individuals (see paragraphs 5.9 to 5.11). AMPs do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a PSC register.

(b) If, and only if, the AMP has exhausted all possible means of identifying the beneficial owner of the corporate customer, and has not succeeded in doing so, or is not satisfied that the individual identified is in fact the beneficial owner, it must take reasonable measures to verify the identity of the senior person in the body corporate responsible for managing it, and keep records in writing of:

- All the actions it has taken to identify the beneficial owner of the body corporate;
- All the actions it has taken in verifying the identifying the senior person in the body corporate; and
- Any difficulties the AMP has encountered in doing so.

Other considerations

Regulation 33(1)(g)

5.115 The standard evidence is likely to be sufficient for most corporate customers. If, however, the customer or transaction is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, its business or its location, or because of the proposed features of the transaction – the AMP must, on a risk-sensitive basis, apply EDD measures, including enhanced monitoring for customers with whom the AMP has a business relationship (see paragraphs 5.2 and 5.4). For example, the AMP will need to decide whether it should require additional identity information to be provided and/or verified (see paragraphs 5.156ff and 5.213/214).

5.116 Higher risk corporate customers may also be, among others, smaller and more opaque entities, with little or no industry profile and those in less transparent jurisdictions, taking account of issues such as their size, industry profile, industry risk.

Bearer shares

5.117 Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s). Companies that issue bearer shares are frequently incorporated in high risk jurisdictions. AMPs should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner.

5.118 As a minimum, these procedures should require an AMP to obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the AMP if the shares are transferred to another party. Depending on its risk assessment of the client, the AMP may consider it appropriate to have this undertaking certified by an accountant, lawyer or equivalent, or even to require that the shares be held by a named custodian, with an undertaking from that custodian that the AMP will be notified of any changes to records relating to these shares and the custodian.

Partnerships and unincorporated bodies

5.119 Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.

Regulation 5(3)

5.120 The beneficial owner of a partnership (other than a limited liability partnership) is any individual who ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercise ultimate control over the management of the partnership.

For example, if no individual owns or controls more than 25% of the capital or profits of the partnership, or of the voting rights in the partnership, AMPs should use judgement in determining whether an individual owning or controlling a lower percentage exercises effective control.

Obtain standard evidence

5.121 The AMP should obtain the following standard evidence in relation to the partnership or unincorporated association:

- full name
- address of principal place of business
- names of all partners/principals who exercise control over the management of the partnership
- names of individuals who own or control over 25% of its capital or profit, or of its voting rights

5.122 Given the wide range of partnerships and unincorporated businesses, in terms of size, reputation and numbers of partners/principals, AMPs need to make an assessment of where a particular partnership or business lies on the associated risk spectrum.

Regulation 28(18)

5.123 The AMP's obligation is to verify the identity of the customer using evidence from a reliable source, independent of the customer. Where partnerships or unincorporated businesses are well known, reputable organisations, with long histories in their industries, and with substantial public information about them and their principals and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be able to provide such reliable and independent evidence. This does not obviate the need to verify the identity of the partnership's beneficial owners.

5.124 As part of the standard evidence, the AMP should know the names of all individual beneficial owners owning or controlling more than 25% of the partnership's capital or profit, or its voting rights or who otherwise exercise control over the management of the partnership. The AMP must take reasonable measures to verify the identity of those individuals (see paragraphs 5.9 to 5.11).

5.125 Other partnerships and unincorporated businesses may have a lower profile. In verifying the identity of such customers, AMPs should primarily have regard to the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals, and follow the guidance set out in paragraphs 5.x – 5.x; where numbers are larger, the AMP should decide whether it should continue to regard the customer as a collection of private individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed (or other evidence in the case of sole traders or other unincorporated businesses), to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked.

5.126 For identification purposes, Scottish partnerships and limited liability partnerships should be treated as corporate customers. For limited partnerships, the identity of general partners should be verified whilst other partners should be treated as beneficial owners.

5.127 AMPs must take appropriate steps to be reasonably satisfied that the person the AMP is dealing with is properly authorised by the customer.

5.128 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language,

appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Other considerations

5.129 Most partnerships and unincorporated businesses are smaller, less transparent, and less well known entities, and are not subject to the same accountability requirements as, for example, companies listed on a regulated market.

5.130 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, AMPs should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, additional precautions should be taken.

5.131 It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the business.

Principals and owners

5.132 Following its assessment of the money laundering or terrorist financing risk presented by the entity, the AMP may decide to verify the identity of one or more of the partners/owners as customers, where they are not already required to do so (see paragraph 5.124 above). In that event, verification requirements are likely to be appropriate for partners/owners who have authority to give the AMP instructions concerning the use or transfer of funds; other partners/owners must be verified as beneficial owners, following the guidance in paragraphs 5.9 to 5.11.

Trusts and foundations

5.133 There is a wide variety of trusts, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs. It is important, in putting proportionate AML/CTF processes into place, and in carrying out their risk assessments, that AMPs take account of the different money laundering or terrorist financing risks that trusts of different sizes, areas of activity and nature of business being conducted, present.

5.134 For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship or transaction with the AMP, in their capacity as trustees of the particular trust or foundation, are the AMP's customers on whom the AMP must carry out full CDD measures. Following a risk-based approach, in the case of a

large, well known and accountable organisation AMPs may limit the trustees considered customers to those who give instructions to the AMP. Other trustees will be verified as beneficial owners, following the guidance in paragraphs 5.9 to 5.11.

5.135 Most trusts are not separate legal persons, and for AML/CTF purposes should be identified as described in paragraphs 5.141 to 5.145.

Regulation 6(1), 42(2)(b)

5.136 The ML Regulations specify that a beneficial owner of a relevant trust means each of the following

- the settlor;
- the trustees;
- the beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates.

Regulation 6(3)

5.137 In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out in paragraph 5.136.

Regulation 42(2)(b)

5.138 For the vast majority of relevant trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the ML Regulations), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution.

Regulation 6(7),(8)

5.139 In relation to a legal entity or legal arrangement which is not a trust the beneficial owners (see paragraph 5.137) are:

- any individual who benefits from the property of the entity or arrangement;
- where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates;
- any individual who exercises control over the property of the entity or arrangement.

5.140 Where an individual is the beneficial owner of a body corporate which benefits from, or exercises control over, the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

Obtain standard evidence

5.141 In respect of trusts, the AMP should obtain the following information:

- Name of the settlor
- Full name of the trust
- Nature, purpose and objects of the trust (e.g., discretionary, testamentary, bare)
- Country of establishment
- Names of all trustees
- Names of any beneficiaries (or, when relevant and as set out in paragraph 5.136, a description of the class of beneficiaries)

- Name of any protector or controller

Regulation 28(2), (4)(c)

5.142 The identity of the trust must be verified on the basis of documents or information obtained from a reliable source which is independent of the customer. This may require sight of relevant extracts from the trust deed, or reference (subject to paragraph 5.144) to an appropriate register in the country of establishment. The AMP must take reasonable measures to understand the ownership and control structure of the trust.

Beneficial owners

Regulation 6(1)(a)(b)

5.143 The ML Regulations specify that the trustees, beneficiaries and settlor of a trust are beneficial owners. In exceptional cases where persons other than trustees, the settlor and beneficiaries exercise control over the trust property, they are to be considered as beneficial owners. Examples of such persons may include trust protectors.

Regulation 28(9)

5.144 The identities of other beneficial owners (e.g., certain beneficiaries), either individuals or a class, as appropriate, must also be verified (see paragraphs 5.9 to 5.11). AMPs do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a register.

Regulation 6(1)

5.145 Where there is a large number of trustees the AMP may take a risk-based approach to determining those in respect of whom the AMP should carry out full CDD measures. (see paragraphs 5.133ff.)

5.146 AMPs must take appropriate steps to be reasonably satisfied that the person the AMP is dealing with is properly authorised by the customer. Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

5.147 Where a trustee is itself a regulated entity (or a nominee company owned and controlled by a regulated entity), or a company listed on a regulated market, or other type of entity, the identification and verification procedures that should be carried out should reflect the standard approach for such an entity.

Other considerations

5.148 AMPs should make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.149 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in this category, the AMP's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Regulation 33(1)

5.150 Where a situation is assessed as carrying a higher risk of money laundering or terrorist financing, the AMP must carry out a higher level of verification. Information that might be appropriate to ascertain for higher risk situations includes:

- Donor/settlor/grantor of the funds (except where there are large numbers of small donors)
- Domicile of business/activity
- Nature of business/activity
- Location of business/activity (operating address)

Non-UK trusts and foundations

5.151 The guidance in paragraphs 5.133 to 5.150 applies equally to UK based trusts and non-UK based trusts. On a risk-based approach, an AMP will need to consider whether the geographical location of the trust (or any other risk factor) gives rise to additional concerns, and if so, whether they should apply EDD. If the trust is established in a high-risk third country, EDD measures are required.

5.152 A foundation ("Stiftung") is described in the FATF October 2006 *Report on the Misuse of Corporate Vehicles* as follows:

"A foundation (based on the Roman law *universitas rerum)* is the civil law equivalent to a common law trust in that it may be used for similar purposes. A foundation traditionally requires property dedicated to a particular purpose. Typically the income derived from the principal assets (as opposed to the assets themselves) is used to fulfil the statutory purpose. A foundation is a legal entity and as such may engage in and conduct business. A foundation is controlled by a board of directors and has no owners. In most jurisdictions a foundation's purpose must be public. However there are jurisdictions in which foundations may be created for private purposes. Normally, foundations are highly regulated and transparent."

5.153 Foundations feature in a number of EEA member state and other civil law jurisdictions including, notably, Liechtenstein and Panama. The term is also used in the UK and USA in a looser sense, usually to refer to a charitable organisation of some sort. In the UK and USA, entities referred to as foundations will frequently be legal entities rather than legal arrangements.

5.154 The nature of a civil law foundation should normally be well understood by AMPs operating in the jurisdiction under whose laws the foundation has been set up. Where a foundation seeks to undertake a transaction

outside its home jurisdiction, AMPs will need to understand the reasons for doing so and to establish the statutory requirements within the specific home jurisdiction for setting up a foundation. So far as possible, comparable information should be obtained as indicated in paragraph 5.141 for trusts, including the identity of the founder and beneficiaries (who may include the founder), whose identity should be verified as necessary on similar risk-based principles.

5.155 Where the founder's identity is withheld, AMPs will need to exercise caution and have regard to the standing of any intermediary and the extent of assurances that may be obtained from them to disclose information on any parties concerned with the foundation in response to judicial demand in the AMP's own jurisdiction. Liechtenstein foundations, for example, are generally established on a fiduciary basis through a licensed trust company to preserve the anonymity of the founder, but the trust companies are themselves subject to AML laws.

Higher risk/enhanced customer due diligence

Regulation 33(1), (6)

5.156 Where higher risks are identified, AMPs are required take enhanced due diligence measures (EDD), and in respect of customers with whom they have a business relationship, enhanced monitoring, to manage and mitigate the risks. Potentially higher risk situations may be influenced by

- Customer risk factors
- Country or geographic risk factors
- Product, service, transaction or delivery channel risk factors

5.157 Where a customer is assessed as carrying a higher risk, then depending on the circumstances (for example, particular features of the transaction), it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from.

Regulations 33(1), 35

5.158 Categories which have been specifically identified under the ML Regulations as requiring EDD include:

- 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 are established in a high risk third country;

- where the AMP has determined that a customer or potential customer, is a Politically Exposed Person (PEP), or a family member or known close associate of a PEP;
- any case where the AMP discovers that a customer has provided false or stolen identification documentation, and the AMP proposes to continue to deal with that customer;
- any case where a transaction is complex or unusually large;
- any case identified as one where there is a high risk of money laundering or terrorist financing, either by the AMP or in information made available to the AMP by the authorities.

5.159 Where the risks of ML/TF are higher (see paragraphs 1.19-1.24 above), AMPs must conduct enhanced due diligence measures consistent with the risks identified.

(a) In particular, AMPs must:

Regulation 33(5)

- as far as reasonably possible, examine the background and purpose of the transaction; and
- where the AMP has a business relationship with the customer, increase the degree and nature of monitoring of the customer's activity (see paragraphs 5.213/214), in order to determine whether these transactions or activities appear unusual or suspicious.

(b) Examples of other EDD measures that, depending on the requirements of the case, could be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and any beneficial owner
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining the approval of senior management to undertake the transaction
- Requiring settlement to be carried out through an account in the customer's name with a bank subject to similar CDD standards

Regulation 33(1)(f),(4)

5.160 Where EDD measures are required, AMPs must as far as reasonably possible examine the background and purpose of all complex and unusually large transactions, and transactions which have no apparent economic or legal purpose.

5.161 In the case of some situations assessed as high risk, the AMP may wish not to take on, or enter into a transaction with, the customer. This may be the case in relation to particular types of customer, or in relation to customers established in, or transactions to or through, particular high risk countries or geographic areas, or in relation to a combination of other risk factors.

5.162 A decision must be made, on the basis of an assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration must be given to all the information an AMP gathers about a customer; consideration of the overall information held may alter the risk profile of the customer.

5.163 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a low risk of money laundering or terrorist financing does not mean that the customer is not. Staff therefore need to be vigilant in using their experience and common sense in applying the AMP's risk-based criteria and rules.

Politically exposed persons (PEPs)

Regulation 35(3)(a)

5.164 Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to AMPs. PEPs can pose a high money laundering risk because they may be able to abuse their position for private gain. Not all PEPs, however, pose the same money laundering risk; there is a hierarchy depending on country of origin and rank, from higher tier officials to individuals with significant or absolute control over the levers, patronage and resources in a given area. 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. It does, however, put the customer, or the beneficial owner, into a higher risk category. The level of risk associated with any PEP, family member or close associate (and the extent of EDD measures to be applied) must be considered on a case-by-case basis.

Regulation 35(4)(b) 48

5.165 Although the FCA is not responsible for supervising AMPs, it is required to give guidance in relation to the EDD measures required under the ML Regulations in respect of PEPs, their family members and known close associates. The FCA guidance[22] is the only regulatory source, and so will provide a source of useful information for AMPs.

Regulation 35(12)(a)

5.166 A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.

[22] https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

Regulation 35(9)

5.167 Under the definition of a PEP the obligation to apply EDD measures to an individual ceases after he has left office for one year, or for such longer period as the AMP considers appropriate, in order to address risks of ML/TF in relation to that person.

Regulation 35(14)

5.168 Individuals entrusted with prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);
- members of the administrative, management or supervisory boards of State-owned enterprises; and
- directors, deputy directors and members of the board or equivalent function of an international organisation.

These categories do not include middle-ranking or more junior officials.

5.169 Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, AMPs should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Regulation 35(12)(b)

5.170 Family members of a PEP include:

- a spouse or partner of that person;
- children of that person and their spouses or partners; and
- parents of that person.

Regulation 35(12)(c)

5.171 Known close associates of a PEP include:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and
- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

Regulation 35(11)

5.172 EDD measures are no longer obliged to be applied to family members or close associates of a PEP when the PEP is no longer entrusted with a prominent public function, whether or not the period in paragraph 5.167 has expired.

Regulation 35(15)

5.173 For the purpose of deciding whether a person is known to be a close associate of a PEP, AMPs may use information that is reasonably available to them which could include: reliable registers, public domain information such as websites of parliament and governments, reliable news sources and works by reputable pressure groups focused corruption. An AMP may also - but is not required to – use commercial databases.

Regulation 35(1), (5)

5.174 AMPs are required to:

- have in place appropriate risk management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP, or a family member or known close associate of a PEP;
- obtain appropriate senior management approval for entering into a transaction with such a customer; and
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction.

Risk-based procedures

5.175 The nature and scope of a particular market participant's business will generally determine whether the existence of PEPs in their customer base is an issue for the AMP, and whether or not the AMP needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if resources were focused in particular on transactions that are characterised by a high risk of money laundering.

Regulation 35(3) 35(4)(b)

5.176 AMPs should take a proportionate, risk-based and differentiated approach to conducting transactions with PEPs, depending on where they are assessed on the scale of risk.

5.177 Establishing whether individuals qualify as PEPs, and therefore the appropriate level of EDD to carry out, is not always straightforward and can present difficulties. On the face of it, the legal definition is quite explicit, but there is clearly a hierarchy, or continuum, of PEPs, from those who may technically qualify under the definition, but be just above a 'middle ranking or junior official' level, to those who have significant, or even absolute, control over the levers, patronage and resources in any given area or jurisdiction. This process can be particularly difficult when seeking to form a view on the status of close family members, such as children and their spouses, who may in reality be quite distant – or even estranged – from their parent(s) or other PEP-status relative.

Regulation 35(3), (4)

5.178 In order to determine how to assess individual customers for PEP purposes, AMPs' analysis should therefore employ an appropriate risk-based approach, to assess where on the PEP continuum an individual lies. AMPs are under a legal requirement to conduct EDD on PEPs, their family members and known close associates. The levels of money laundering/terrorist financing risk presented will vary on a case-by-case basis. The higher up the risk scale a PEP is, the more extensive the EDD measures that should be carried out. Conversely, in cases lower down

the risk scale, it may be appropriate for AMPs to take less intrusive and less exhaustive EDD measures.

5.179 Where AMPs need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. When using a commercial database, the AMP should understand how the database is populated. Resources such as the Transparency International Corruption Perception Index, which ranks approximately 150 countries according to their perceived level of corruption, may also be helpful in terms of assessing the risk. The IMF, World Bank and some non-governmental organisations also publish relevant reports.

Source of wealth

5.180 It is for each AMP to decide the steps it takes to determine whether a PEP is seeking to undertake a transaction for legitimate reasons.

Regulation 35(5)(b)

5.181 AMPs must take adequate measures to establish the source of wealth and source of funds which are involved in a business relationship or transaction in order to allow the AMP to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures AMPs should take to establish the PEP's source of wealth and the source of funds will depend on the degree of risk associated with the business relationship or transaction, and where the individual sits on the PEP continuum. AMPs should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

5.182 AMPs should, where possible, refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests[23]. AMPs should note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. AMPs should also be aware that some jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts or to hold other office or paid employment.

5.183 For PEPs who are assessed as being higher on the scale of risk, AMPs could, for example, and when conducting source of wealth checks on funds from inheritance, request a copy of the relevant will. Where the wealth/funds of such PEPs originate from the sale of property, AMPs could seek evidence of conveyancing.

Senior management approval

[23] The World Bank has compiled a library on various countries' laws about disclosure of officials' income and assets. See http://publicofficialsfinancialdisclosure.worldbank.org/about-the-library

5.184 Obtaining approval from senior management (see paragraph 5.174) for undertaking a transaction does not necessarily mean obtaining approval from the Board of directors (or equivalent body), but from a higher level of authority from the person seeking such approval. As risk dictates, AMPs should escalate decisions to more senior management levels.

5.185 The appropriate level of seniority for sign off should therefore be determined by the level of increased risk associated with the transaction; and the senior manager approving a PEP transaction should have sufficient seniority and oversight to take informed decisions on issues that directly impact the AMP's risk profile, and not (solely) on the basis that the individual is a PEP. When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the AMP would be exposed to if it entered into that transaction and how well equipped the AMP is to manage that risk effectively.

Lower risk/simplified customer due diligence

5.186 Many customers, by their nature or through what is already known about them by the AMP, carry a lower money laundering or terrorist financing risk. Where an AMP has determined that a customer presents a low risk of money laundering, based on appropriate, documented evidence, reduced CDD measures may be applied. Such customers might include:

- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; and
- Customers with a long-term and active relationship with the AMP.

Regulation 37(1)

5.187 There are other circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the AMP, the AMP may (if permitted by local law or regulation) apply reduced CDD measures. Potentially lower risk situations may be influenced by:

- Customer risk factors
- Country or geographic risk factors
- Product, service, transaction value/frequency or delivery channel risk factors

5.188 Having a lower money laundering or terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures.

5.189 AMPs should not, however, judge the level of risk solely on the nature of the customer or of the transaction. Where, in a particular customer/product combination, *either or both* the customer and the transaction are considered to carry a higher risk of money laundering or terrorist financing, the overall risk of the customer should be considered carefully.

Reliance on third parties

5.190 Sometimes a customer may have contact with two or more AMPs in respect of the same transaction. This can be the case where customers are introduced by one AMP to another, or where several AMPs may be involved in a transaction with the same customer.

5.191 To have several AMPs requesting the same information from the same customer in respect of the same transaction does not help in the fight against financial crime, and adds to the inconvenience of the customer. It is important, therefore, that each AMP with AML/CTF obligations on its customer is clear on the extent to which it can rely upon or otherwise take account of the verification of the customer that another AMP has carried out. Such account must be taken in a balanced way that appropriately reflects the money laundering or terrorist financing risks. Account must also be taken of the fact that some of the AMPs involved may not be UK-based.

Regulation 39

5.192 The ML Regulations expressly permit an AMP to rely on another person to apply any or all of the required CDD measures, provided that the other person is listed in Regulation 39(3) – see paragraph 5.194. The relying AMP, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated. The relying AMP also still has to carry out its own customer risk assessment.

5.193 For example:

- where an AMP (AMP A) enters into a transaction for the underlying customer of another market participant (AMP B), for example by accepting instructions from the customer given through AMP B; or
- AMP A and AMP B both act for the same customer in respect of a transaction,

AMP A may rely on AMP B to carry out CDD measures, while remaining ultimately liable for compliance with the ML Regulations.

Regulation 39(3)

5.194 In this context, AMP B must be:

(1) a person who carries on business in the UK who is subject to the requirements of the ML Regulations; or

(2) a person who carries on business in another EEA State who is subject to, and supervised for compliance with, the requirements of 4MLD; or

(3) a person who carries on business in a third country who is subject to, and supervised for compliance with, CDD and record keeping requirements equivalent to those laid down in 4MLD.

Regulation 39(4)

5.195 An AMP may not rely on a third party established in a country which has been identified by the EC as a high risk third country.

Regulation 39(2)(b) 40(6)

5.196 The AMP must enter into arrangements with the AMP (third party) being relied on which:

- Enable the AMP to obtain from the third party immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the customer or beneficial owner;
- Require the third party to retain copies of the data and documents referred to for the periods set out in Regulation 40 (see paragraphs 7.11 and 7.18).

Regulation 39(7)

5.197 Separately from reliance, an AMP is permitted to apply CDD measures by means of an agent or an outsourcing service provider, provided that the arrangements between the AMP and the agent or service provider make clear that the AMP remains liable for any failure to apply the CDD measures.

Basis of reliance

5.198 For one AMP to rely on verification carried out by another AMP, the verification that the AMP being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on the basis of simplified due diligence having been carried out, or any other exceptional form of verification. In order to judge whether to rely on another AMP, the relying AMP must know what CDD measures have been carried out.

5.199 AMPs may also only rely on verification actually carried out by the AMP being relied upon. An AMP that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another AMP.

5.200 Whether an AMP wishes to place reliance on a third party will be part of the AMP's risk-based assessment of the particular customer and transaction, which, in addition to confirming what CDD measures have been carried out and the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available;
- the nature of the customer, of the transaction and the sums involved;

- any adverse experience of the other AMP's general efficiency in business dealings;
- any other knowledge that the AMP has regarding the standing of the AMP to be relied upon.

5.201 The assessment as to whether or not an AMP should accept confirmation from a third party that appropriate CDD measures have been carried out on a customer will be risk-based, and cannot be based simply on a single factor.

5.202 In practice, the AMP relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified;
- the level of CDD that has been carried out; and
- confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

5.203 The third party has no obligation to provide such confirmation to the AMP, and may choose not to do so. In such circumstances, or if the AMP decides that it does not wish to rely upon the third party, then it must carry out its own CDD measures on the customer.

5.204 For an AMP to confirm that it has carried out CDD measures in respect of a customer is a serious matter. Confirmation must not be given on the basis of a generalised assumption that the AMP's systems have operated effectively. There has to be awareness that the appropriate steps have in fact been taken in respect of the customer that is the subject of the confirmation.

5.205 An AMP must also document the steps taken to confirm that the AMP relied upon satisfies the requirements in Regulation 39(3). This is particularly important where the AMP relied upon is situated outside the EEA.

Use of pro-forma confirmations

Regulation 39 (3)

5.206 Whilst an AMP may be able to place reliance on another party to apply all or part of the CDD measures under Regulation 39(3) (see paragraph 5.192), it may still wish to receive, as part of its risk-based procedures, a written confirmation from the third party. This may also be the case, for example, when an AMP is entering into a new relationship with the third party. Confirmations can be particularly helpful when dealing with third parties located outside of the UK, where it is necessary to confirm that the relevant records will be available (see 5.196).

5.207 Pro-forma confirmations may be used for customer identification and verification.

Situations which are not reliance

(i) One AMP acting solely as introducer

5.208 At one end of the spectrum, a third party may act solely as an introducer between the customer and the AMP entering into the transaction, and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the AMP, and has no relationship with either of these parties that would require it to apply CDD measures.

5.209 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, any identification and verification obligations under the ML Regulations lie with the AMP.

(ii) Where the intermediary is the agent of the customer

5.210 From the point of view of an AMP, the ability to rely on, or to take account of CDD measures carried out by, an intermediary as agent of the customer, is influenced by a number of factors. The intermediary may be subject to the ML Regulations, or otherwise to the EU Fourth Money Laundering Directive, or to similar legislation in an assessed low risk jurisdiction. It may be regulated; it may be based in the UK, elsewhere within the EU, or in a country or jurisdiction outside the EU, which may or may not be a FATF member.

Regulation 37(1)

5.211 Depending on jurisdiction, where the intermediary is carrying on appropriately regulated business, and is acting on behalf of the customer, and the AMP determines that the situation presents a low degree of risk of ML/TF, the art market participant may decide to carry out simplified due diligence measures on both the intermediary and the underlying customer.

5.212 Where an AMP cannot apply simplified due diligence to the intermediary it is obliged to carry out CDD measures on the intermediary and, as the intermediary acts for another, on the underlying customer.

Monitoring customer activity

The requirement to monitor customers' activities

Regulation 28(11)

5.213 Where an AMP has a business relationship with a customer (but not otherwise), it must conduct ongoing monitoring of the customer's activity. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the AMP's knowledge of the customer, his business and risk profile;
- Ensuring that the documents or information obtained for the purposes of applying customer due diligence are kept up to date.

5.214 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps AMPs know their customers, assist them to assess risk and provides greater assurance that the AMP is not being used for the purposes of financial crime.

6. Reporting suspicions

General legal and regulatory obligations

POCA ss 330, 331
Terrorism Act s 21A

6.1 All persons in the regulated sector (which includes AMPs) are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they *know* or
- where they *suspect* or
- where they *have reasonable grounds for knowing or suspecting*

that a person is engaged in, or attempting, money laundering or terrorist financing.

Minimum requirements

- Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that a terrorist finance offence may be committed.
- The nominated officer must consider all internal reports. The nominated officer must make a report to the National Crime Agency (NCA) as soon as it is practical to do so, **even if no transaction takes place,** if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or financing terrorism.
- The AMP must consider whether it needs to seek a defence to a money laundering or terrorist financing offence (consent) from the NCA before proceeding with a suspicious transaction or entering into arrangements.
- It is a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.

Regulation 19(4)(d)
POCA s 330

6.2 In order to provide a framework within which suspicion reports may be raised and considered:

- each AMP must ensure that any member of staff reports to the AMP's nominated officer, where they have grounds for knowledge or suspicion that a person or customer is engaged in, or attempting, money laundering or terrorist financing;

Regulation 21(5)

- the AMP's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;

Regulation 24

- AMPs should ensure that staff are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

POCA, s 331
Terrorism Act s 21A

6.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to the NCA. Under POCA, the nominated officer is required to make a report to the NCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

6.4 A sole trader with no employees who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of his, or the person on whose behalf the customer is acting, is or has been engaged in, or attempting, money laundering or terrorist financing, must make a report promptly to the NCA.

POCA ss 333A -334
Terrorism Act ss 21D-H, 39

6.5 It is a criminal offence for any person, following a disclosure to a nominated officer or to the NCA, to release information that might 'tip off' another person that a disclosure has been made if the disclosure is likely to prejudice an investigation, if the information released came to that person in the course of a business in the UK regulated sector. It is also an offence for a person to disclose that an investigation into allegations that an offence has been committed is being contemplated or is being carried out if the disclosure is likely to prejudice that investigation and the information on which the disclosure is based came to the person in the course of a business in the regulated sector. It is also an offence for a person to disclose to another anything which is likely to prejudice an investigation resulting from a disclosure, or where the person knows or has reasonable cause to suspect that a disclosure has been or will be made.

Financial sanctions legislation

6.6 It is a criminal offence to make funds available to those persons or entities listed as the targets of financial sanctions legislation. There is also a requirement to report to the Office of Financial Sanctions Implementation (OFSI) both details of any funds frozen, and where AMPs have knowledge or suspicion that a customer of the AMP or a person with whom the AMP has had business dealings is a listed person or entity, a person acting on behalf of a listed person or entity or has committed an offence under the sanctions legislation.

Attempted offences

POCA, s 330

Terrorism Act s21A(2)

6.7 POCA and the Terrorism Act provide that a disclosure must be made where there are grounds for suspicion that a person is engaged in money laundering or terrorist financing. The definition of "money laundering" in POCA includes an attempt to commit an offence under s327-329 of POCA. Similarly, under the Terrorism Act a disclosure must be made where a person has knowledge or suspicion that 'another person had committed *or attempted to commit* an offence under any of the sections 15-18'. There is no duty under s330 of POCA or s21A of the Terrorism Act to disclose information about the person who unsuccessfully attempts to commit fraud. This is because the attempt was to commit fraud, rather than to commit an offence under those Acts.

6.8 However, as soon as the AMP has reasonable grounds to know or suspect that any benefit has been acquired, whether by the fraudster

himself or by any third party, so that there is criminal property or terrorist property in existence, then, subject to paragraph 6.9, knowledge or suspicion of money laundering or terrorist financing must be reported to the NCA. Who carried out the criminal conduct, and who benefited from it, or whether the conduct occurred before or after the passing of POCA, is immaterial to the obligation to disclose, but should be reported if known.

What is meant by "knowledge" and "suspicion"?

POCA, s 330 (2),(3), s 331 (2), (3) Terrorism Act ss21A, 21ZA, 21ZB

6.9 Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual *in fact* knew that a person was engaged in money laundering. That said, knowledge can be *inferred* from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have come to the AMP (or to the member of staff) in the course of business, or (in the case of a nominated officer) as a consequence of a disclosure under s 330 of POCA or s 21A of the Terrorism Act. Information that comes to the AMP or staff member in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should staff choose to do so, or are obligated to do so by other parts of these Acts.

6.10 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:

> *"A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not";* and
>
> *"Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."*

6.11 A transaction which appears unusual is not necessarily suspicious. Many customers will, for perfectly good reasons, have an erratic pattern of transactions. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

6.12 A member of staff, including the nominated officer, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

What is meant by "reasonable grounds to know or suspect"?

POCA, s 330 (2)(b), s 331 (2)(b) Terrorism Act s 21A

6.13 In addition to establishing a criminal offence when suspicion or actual knowledge of money laundering/terrorist financing is proved, POCA and the Terrorism Act introduce criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering/terrorist financing. This

introduces an objective test of suspicion. Reasonable grounds for suspecting are likely to depend upon particular circumstances. The AMP may take into account such factors as the nature/origin of the transaction, the amounts or values involved, their intended movement and destination, how the funds or asset(s) came into the customer's possession, whether the customer(s) and/or the owners of the asset(s) (if different) appear to have any links with criminals/criminality, terrorists, terrorist groups or sympathisers, whether in the UK or overseas.

6.14 To defend themselves against a charge that they failed to meet the objective test of suspicion, staff of AMPs would need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach, to know the customer and the rationale for the transaction or instruction. It is important to bear in mind that, in practice, members of a jury may decide, with the benefit of hindsight, whether the objective test has been met.

Internal reporting

Regulation 19(4)(d)
POCA s 330(5)

6.15 The obligation to report to the nominated officer within the AMP where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees. All AMPs therefore need to ensure that all relevant employees know who they should report suspicions to.

6.16 Once an employee has reported his suspicion in an appropriate manner to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

6.17 Until the nominated officer advises the member of staff making an internal report that no report to the NCA is to be made, further transactions in respect of that customer should be reported to the nominated officer as they arise.

External reporting

Regulation 19(4)(d)
POCA, s 331
Terrorism Act, s 21A

6.18 The AMP's nominated officer must report to the NCA any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to him.

POCA, s 339

6.19 POCA provides that the Secretary of State may by order prescribe the form and manner in which a disclosure under s330, s331, s332 or s338 may be made.

6.20 The NCA prefers that SARs are submitted electronically via the secure internet system SAR Online, or via a dedicated bulk reporting facility. Information about access to and guidance on the use of SAR Online can be found at http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars

6.21 In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and law enforcement agencies should be controlled through, or reported back to a single contact point, which will typically be the nominated officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the AMP's legal or compliance department.

6.22 AMPs should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer. As there is no obligation to collect this information (other than in very specific cases), an AMP may not hold these details for its customers; where it has obtained this information in the course of normal business, however, it would be helpful to include it as part of a SAR made by the AMP. The NCA's website (http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars) contains guidance on completing SARs in a way that gives most assistance to law enforcement. In particular, the NCA has published a glossary of terms, and find it helpful if AMPs use these terms when completing a SAR. NCA also publish, from time to time, guides to reporting entities.

Financial sanctions legislation

6.23 AMPs must report to OFSI where the AMP has knowledge or a suspicion that the financial sanctions measures have been or are being contravened, or that a customer is a listed person or entity, or a person acting on behalf of a listed person or entity. The AMP may also need to consider whether the AMP has an obligation also to report under POCA or the Terrorism Act.

Where to report

6.24 To avoid committing a failure to report offence, nominated officers must make their disclosures to the NCA. The national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UKFIU within the NCA.

6.25 The UKFIU address is PO Box 8000, London, SE11 5EN and it can be contacted during office hours on: 020 7238 8282. Urgent disclosures, i.e., those requiring consent, should be transmitted electronically over a previously agreed secure link or, if secure electronic methods are not available, by fax, as specified on the NCA website at www.nationalcrimeagency.gov.uk. Speed of response is assisted if the appropriate consent request is clearly mentioned in the title of any faxed report (http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars).

6.26 To avoid committing a failure to report offence under financial sanctions legislation, AMPs must make their reports to HM Treasury. The relevant unit is the Office of Financial Sanctions Implementation, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. Reports can be submitted electronically at ofsi@hmtreasury.gsi.gov.uk and the Unit can be contacted by telephone on 020 7270 5454.

Sanctions and penalties

POCA s334
Terrorism Act s21A

6.27 Where a person fails to comply with the obligation under POCA or the Terrorism Act to make disclosures to a nominated officer and/or the NCA as soon as practicable after the information giving rise to the knowledge or suspicion comes to the member of staff, an AMP is open to criminal prosecution or regulatory censure. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

Financial sanctions legislation

6.28 Where an AMP fails to comply with the obligations not to make funds available to listed persons or entities or to report knowledge or suspicion, it is open to prosecution.

Consent under POCA

POCA s 336

6.29 Reporting before or reporting after the event are not equal options which an AMP can choose between. Where a customer instruction is received prior to a transaction taking place, or there are grounds for knowledge or suspicion that the transaction or the funds/property involved, may relate to money laundering, a report must be made to the NCA and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to permit a transaction or activity to proceed within the seven working day notice period from the working day following the date of disclosure, unless the NCA gives consent.

POCA ss 330 (6)(a), 331(6), 338 (3)(b)

6.30 When delaying a transaction which gives rise to concern would lead to a breach of a contractual obligation, the nominated officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, POCA provides a defence from making a report where there is a reasonable excuse for not doing so. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

6.31 When a defence request is sought to undertake a future transaction, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if electronic methods are not available, faxed to the NCA UKFIU Consent Desk immediately the suspicion is identified. Defence requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the NCA website www.nationalcrimeagency.gov.uk. The Consent Desk will apply NCA policy to each submission, carrying out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing AMP will be informed of the decision by telephone, and be given a reference number, which should be recorded. A formal letter will follow.

POCA, s 335, 336A, 336C

6.32 In the event that the NCA does not refuse a defence request within seven working days following the working day after the disclosure is

made, the AMP may process the transaction or activity, subject to normal commercial considerations. If, however, a defence request is refused within that period, a restraint order must be obtained by the authorities within a further 31 calendar days (the moratorium period) from the day the request is refused, if they wish to prevent the transaction going ahead after that date. The moratorium period may be extended, on application by the authorities, by up to 31 days at a time, to a maximum of 186 further days in total. In cases where a defence request is refused, the law enforcement agency refusing the request should be consulted to establish what information can be provided to the customer.

POCA, s 335(1)(b)

6.33 Granting of a defence request by the NCA (referred to as a 'notice' in POCA), or the absence of a refusal of such a request within seven working days following the working day after the disclosure is made, provides the person handling the transaction or carrying out the activity, or the nominated officer of the reporting AMP, with a defence against a possible later charge of laundering the proceeds of crime in respect of that transaction or activity if it proceeds.

Tipping off, and prejudicing an investigation

POCA s 333A (1), (3)
Terrorism Act, s 21D

6.34 POCA and the Terrorism Act each contains two separate offences of tipping off and prejudicing an investigation. The first offence relates to disclosing that an internal or external report has been made; the second relates to disclosing that an investigation is being contemplated or is being carried out. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions precedent for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector.

POCA ss 333A (1), 333D(3)
Terrorism Act,
ss 21D(1), 21G(3)

6.35 Once an internal or external suspicion report has been made, it is a criminal offence for anyone to disclose information about that report which is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures, and should not give rise to the tipping off offence.

POCA, ss 333A(3), 333D(4)
Terrorism Act,
ss 21D(3), 21G(4)

6.36 Where a money laundering investigation is being contemplated, or being carried out, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice that investigation. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act.

Permitted disclosures

POCA s 333D(1) Terrorism Act, s 21G(1)

6.37 An offence is not committed if the disclosure is made to the HMRC (or other relevant supervisor) for the purpose of:

- the detection, investigation or prosecution of a criminal offence (whether in the UK or elsewhere);
- an investigation under POCA; or
- the enforcement of any order of a court under POCA.

POCA, s 333B(1) Terrorism Act, Ss 21A, 21E(1)

6.38 An employee, officer or partner of an AMP does not commit an offence under POCA, s333A, or the Terrorism Act, s 21A, if the disclosure is to an employee, officer or partner of the same AMP.

POCA, ss 335, 336 Terrorism Act, ss21ZA, ZB

6.40 The fact that a transaction is notified to the NCA before the event, and the NCA does not refuse consent within seven working days following the day after the authorized disclosure is made, or a restraint order is not obtained within the 31 day (or extended) moratorium period, does not alter the position so far as 'tipping off' is concerned.

6.41 This means that an AMP:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from the NCA;
- cannot later – unless law enforcement/the NCA agrees, or a court order is obtained permitting disclosure – tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act; and
- cannot tell the customer that law enforcement is conducting an investigation.

Data Protection - Subject Access Requests, where a suspicion report has been made (or is about to be made)

6.42 The data protection legislation, i.e. the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) governs the processing of information relating to individuals, including obtaining, holding, use or disclosure of information. Personal data obtained by a business under the ML Regulations may only be processed for the prevention of money laundering and terrorist financing or where use of the data is allowed by other legislation or after obtaining the consent of the data subject. The processing of personal data in accordance with the ML Regulations is lawful and necessary for the prevention of money laundering or terrorist financing and is for the performance of a task carried out in the public interest.

6.43 Occasionally, a Subject Access Request under the Data Protection Act will include within its scope one or more money laundering/terrorist financing reports which have been, or are about to be, submitted in relation to that customer. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it. However,

all such requests must be carefully considered on their merits, taking appropriate legal advice.

6.44 To guard against a tipping-off offence, nominated officers should ensure that no information relating to SARs is released to any person without the nominated officer's authorisation. Further consideration may need to be given to suspicion reports received internally that have not been submitted to the NCA. A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off.

7. Record keeping

Regulation 19(1)(a)

7.1 Record keeping is an essential component of the audit trail that the ML Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Regulation 18(4), 19(1)(b), 39(2)(b)

7.2 As well as obligations for record keeping in relation to customer identification, and transactions with customers, AMPs are required to document their risk assessment, and their policies, controls and procedures. An AMP is also required to have arrangements with any third party on which they rely to apply customer due diligence measures.

Regulation 40

7.3 AMPs must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

Minimum requirements

AMPs must retain:

- copies of the evidence obtained to satisfy customer due diligence obligations and details of customer transactions for at least five years after the end of the business relationship
- details of occasional transactions for at least five years from the date of the transaction
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make a suspicious activity report
- copies of the evidence obtained if the AMP is relied on by another AMP to carry out customer due diligence, for five years from the date that the third party's relationship with the customer ends, the agreement should be in writing

AMPs must also maintain:

- a written record of its risk assessment
- a written record of its policies, controls and procedure
- a written record of the what it has done to make staff aware of the money laundering and terrorist financing legislation and related data protection requirements, as well as the training given to staff

What records have to be kept?

7.4 The precise nature of the records required is not specified in legislation. The objective is to ensure that an AMP meets its obligations and that, in so far as is practicable, in any subsequent investigation the AMP can provide the authorities with its section of the audit trail.

7.5 The AMP's records should cover:

- Customer information
- Transactions
- Internal and external suspicion reports
- Nominated officer's annual (and other) reports
- Information not acted upon
- Training and compliance monitoring
- Information about the effectiveness of training

Customer information

Regulation 40(2)

7.6 In relation to the evidence of a customer's identity, AMPs must keep a copy of any documents or information it obtained to satisfy the CDD measures required under the ML Regulations. Where an AMP has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept.

7.7 An AMP may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

7.8 The Home Office current guidance on copying passports is available at http://www.nationalarchives.gov.uk/documents/information-management/reproduction-british-passport.pdf

Regulation 40(3)(b)(ii)

7.9 Where relevant, records of identification evidence must be kept for a period of five years after the business relationship with the customer has ended.

Regulation 40(5)

7.10 Upon the expiry of the five year period referred to in paragraph 7.9, AMPs must delete any personal data unless:

- the AMP is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the AMP has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

Regulation 40(6)

7.11 An AMP who is relied on by another AMP for the purposes of customer due diligence in relation to a customer with whom the AMP has a business relationship must keep the records referred to in paragraph 7.6 for five years from the ending of the business relationship with the customer.

7.12 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the nominated officer and to all areas that have contact with the customer, and be available on request, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them.

Transactions

7.13 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the AMP's records. Transaction records in support of entries in the accounts, in whatever form they are used, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect customer.

Regulation 40(3)(a)(b)(i)

7.14 Records of all transactions relating to a customer must be retained for a period of five years from:

- where the records relate to an occasional transaction, the date when the transaction is completed; or
- in other cases, the date the business relationship ended.

Regulation 40(4)

But: an AMP is not required to retain records relating to transactions occurring in a business relationship for more than 10 years.

Regulation 40(5)

7.15 Upon the expiry of the period referred to in paragraph 7.14, AMPs must delete any personal data unless:

- the AMP is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the AMP has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

Internal and external reports

7.16 An AMP should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering, but has not made a report to the NCA, a record of the other material that was considered.

7.17 In addition, copies of any SARs made to the NCA should be retained.

7.18 Records of all internal and external reports should be retained for at least five years from the date the report was made.

Other

7.19 An AMP's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring -

- reports by the nominated officer to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

Form in which records have to be kept

7.20 Most AMPs will have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- by way of original documents;
- by way of photocopies of original documents;
- on microfiche;
- in scanned form;
- in computerised or electronic form.

7.21 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

Location

7.22 The ML Regulations do not state where relevant records should be kept, but the overriding objective is for AMPs to be able to retrieve relevant information without undue delay.

7.23 Where identification records are held outside the UK, it is the responsibility of the UK AMP to ensure that the records available do in fact meet UK requirements. Subject to secrecy or data protection legislation, there should be no restriction to access to the records either by the UK AMP freely on request, or by UK law enforcement agencies under their statutory powers, under a court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the UK.

7.24 AMPs should take account of the scope of AML/CTF legislation in other countries, and should ensure that group records kept in other countries that are needed to comply with UK legislation are retained for the required period.

7.25 There can sometimes be tension between the provisions of the ML Regulations and data protection legislation; the nominated officer must have due regard to both sets of obligations.

Sanctions and penalties

Regulation 86(1)

7.26 Where the record keeping obligations under the ML Regulations are not observed, an AMP is open to prosecution, including imprisonment for up to two years and/or a fine, or regulatory censure.