CHAPTER 5

CUSTOMER DUE DILIGENCE

- **Relevant UK law/regulation**
  - Regulations 4-6, 27-38
  - POCA ss 330 – 331, 334(2), 342
  - Terrorism Act
  - Counter-terrorism Act 2008, Schedule 7
  - Financial sanctions legislation
- **Customers that may not be dealt with**
  - UN Sanctions resolutions 1267 (1999), 1373 (2001), 1333 (2002), 1390 (2002) and 1617 (2005)
  - EC Regulation 2580/2001, 881/2002 (as amended), 423/2007 and 1110/2008
  - EU Regulation 2016/1686
  - Terrorism Act, 2000, Sch 2
  - Terrorism (United Nations Measures) Orders 2006 and 2009
  - Al-Qa'ida and Taliban (United Nations Measures) Order 2006
  - HM Treasury Sanctions Notices and News Releases
- **Regulatory regime**
  - SYSC 6.1.1 R, 6.3.7(5) G
  - FCA Financial Crime Guide
  - FCA PEPs guidance
- **Other material pointing to good practice**
  - FATF Recommendations
  - FATF Guidance on the risk-based approach: High level principles and procedures
  - Basel paper – *Sound management of risks related to money laundering and financing of terrorism*
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
  - ESA Risk Factor Guidelines

- **Core obligations**
  - Must carry out prescribed CDD measures for all customers not covered by exemptions
  - Must have systems to deal with identification issues in relation to those who cannot produce the standard evidence
  - Must take a risk based approach when applying enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, specifically in respect of PEPs and correspondent relationships
  - Some persons/entities must not be dealt with
  - Must have specific policies in relation to the financially (and socially) excluded
  - If satisfactory evidence of identity is not obtained, the business relationship must not proceed further
  - Must have some system for keeping customer information up to date

5.1 Meaning of customer due diligence measures and ongoing monitoring

5.1.1 The ML Regulations 2017 specify CDD measures that are required to be carried out, and the timing, as well as actions required if CDD measures are not carried out. The Regulations then describe circumstances in which limited CDD measures are permitted (referred to as 'Simplified Due Diligence'), and those customers and circumstances where enhanced due

diligence is required. Provision for reliance on other regulated firms in the carrying out of CDD measures are then set out.

5.1.2 Schedule 7 to the Counter-terrorism Act 2008 gives HM Treasury power to require firms, in particular circumstances, to carry out enhanced CDD and monitoring. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk. Guidance on complying with directions issued by HM Treasury under CTA 2008, Schedule 7 is given in Part III, section 5.

5.1.3 This chapter therefore gives guidance on the following:

- The meaning of CDD measures (5.1.5 – 5.1.15)
- Timing of, and non-compliance with, CDD measures (5.2.1 – 5.2.13)
- Application of CDD measures (section 5.3)
- Simplified due diligence (section 5.4)
- Enhanced due diligence (section 5.5)
- Reliance on third parties and multipartite relationships (section 5.6)
- Monitoring customer activity (section 5.7)

Regulation 28(12),(16)

5.1.4 Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

What is customer due diligence?

Regulation 28(1), (2)

5.1.5 The CDD measures that must be carried out involve:

(a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff**);**
(b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff)**;** and
(c) assessing, and where appropriate obtaining information on, the purpose and intended nature of the business relationship or transaction(see paragraphs 5.3.23ff**)**.

Regulation 28(4)(c), (5)

5.1.6 Where the beneficial owner is a legal person (other than a company listed on a regulated market), trust, company, foundation or similar legal arrangement, firms must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement.

5.1.7 Working out who is a beneficial owner may not be a straightforward matter. Different rules apply to different forms of entity (see paragraphs 5.3.8ff).

Regulations 33-38

5.1.8 For some business relationships, determined by the firm to present a low degree of risk of ML/TF, simplified due diligence (SDD) may be applied; in the case of higher risk situations, and specifically in relation to PEPs or correspondent relationships with non-EEA respondents, enhanced due diligence (EDD) measures must be applied on a risk sensitive basis.

- for guidance on applying SDD see section 5.4

- for guidance on applying EDD see section 5.5

What is ongoing monitoring?

Regulation 28(11)

5.1.9 Firms must conduct ongoing monitoring of the business relationship with their customers (see paragraphs 5.7.1ff), including the scrutiny of transactions undertaken throughout the course of the relationship and keeping CDD information up to date. This is a separate, but related, obligation from the requirement to apply CDD measures.

Why is it necessary to apply CDD measures and conduct ongoing monitoring?

Regulations 27, 28
POCA, ss 327-334
Terrorism Act s 21A

5.1.10 The CDD and monitoring obligations on firms under legislation and regulation are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

5.1.11 Firms also need to know who their customers are to guard against fraud, including impersonation fraud, and the risk of committing offences under POCA and the Terrorism Act, relating to money laundering and terrorist financing.

Criminal Finances Act

5.1.12 Tax evasion is a predicate offence leading to money laundering. Failing to report knowledge or suspicions relating to such an activity is an offence committed by a firm.

5.1.13 Firms therefore need to carry out customer due diligence, and monitoring, for two broad reasons:

- to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and
- to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.

5.1.14 It may often be appropriate for the firm to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business or activities in order to assess the extent to which his transactions and activity undertaken with or through the firm is consistent with that business.

Other material, pointing to good practice

5.1.15 FATF, the Basel Committee, IAIS and IOSCO have issued recommendations on the steps that should be taken to identify customers. FATF has also published guidance on high level principles and procedures on the risk-based approach. The Basel Committee's recommendations comprise a set of guidelines on the *Sound management of risks relating to money laundering and financing of terrorism*. Although the Basel paper is addressed to banks, the IAIS Guidance Paper 5 to insurance entities, and IOSCO's Principles paper to the securities industry, their principles are worth considering by providers of other forms of financial services. These recommendations are available at: www.fatf-gafi.org; www.bis.org; www.iaisweb.org; www.iosco.org. Where relevant, firms are encouraged

to use these websites to keep up to date with developing industry guidance from these bodies. The private sector Wolfsberg Group has also issued relevant material, see www.wolfsberg-principles.com.

5.2 Timing of, and non-compliance with, CDD measures

Regulation 27(1) 5.2.1 A firm must apply CDD measures when it does any of the following:

(a) establishes a business relationship;
(b) carries out an occasional transaction;
(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.

Timing of verification

Regulation 30(2) 5.2.2 **General rule**: The verification of the identity of the customer and, where applicable, the beneficial owner, must, subject to the exceptions referred to below, take place before the establishment of a business relationship or the carrying out of a transaction.

Regulation 30(3) 5.2.3 **Exception if necessary not to interrupt normal business and there is little risk:** In any other case, verification of the identity of the customer, and where there is one, the beneficial owner, may be completed during the establishment of a business relationship if

(a) this is necessary not to interrupt the normal conduct of business and
(b) there is little risk of money laundering or terrorist financing occurring

provided that the verification is completed as soon as practicable after contact is first established.

Regulation 30(4),(5) 5.2.4 **Exception when opening a account:** The verification of the identity of a customer (or beneficial owner, if there is one) opening an account may take place after the account (including an account which permits transactions in transferable securities) has been opened, provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed.

Regulation 30(6),(7) 5.2.5 **Other exceptions:** Where a firm is required to apply CDD measures in the case of a trust, a legal entity (other than a body corporate) or a legal arrangement (other than a trust), and the beneficiaries of that trust, entity or arrangement are designated as a class, or by reference to particular characteristics, the firm must establish and verify the identity of the beneficiary before –

- any payment is made to the beneficiary, or
- the beneficiary exercises its vested rights in the trust, entity or legal arrangement.

Requirement to cease transactions, etc

Regulation 31(1)

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm

(a) must not carry out a transaction through a bank account with or on behalf of the customer;
(b) must not establish a business relationship or carry out a transaction with the customer otherwise than through a bank account;
(c) must terminate any existing business relationship with the customer;
(d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.

5.2.7 Firms should always consider whether an inability to apply CDD measures is caused by the customer not possessing the 'right' documents or information. In this case, the firm should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the firm should consider whether there are any circumstances which give grounds for making a report.

Regulation 31(1), (2)

5.2.8 If the firm concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be made to the NCA (see Chapter 6). The firm must then retain the funds until consent has been given to return the funds to the source from which they came.

Regulation 31(2)

5.2.9 If the firm concludes that there are no grounds for making a report, it will need to decide on the appropriate course of action. This may be to retain the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or to return the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

Electronic transfer of funds

EC Regulation 2015/847

5.2.10 To implement FATF Recommendation 16, the EU adopted Regulation 2015/847, which came into force on 26 June 2017, and is directly applicable in all member states. The Regulation requires that payment services providers (PSPs) must include certain information in electronic funds transfers and ensure that the information is verified. The core requirement is that the payer's name, address and account number, and the name and payment account number of the payee, are included in the transfer, but there are a number of permitted exemptions, concessions and variations. For guidance on how to meet the obligations under the Regulation, see Part III, Specialist Guidance 1: *Wire transfers*.

5.2.11 The Regulation includes (among others) the following definitions:

- 'Payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or where there is no payment account, that gives a transfer of funds order.
- 'Payee' means a person that is the intended recipient of the transfer of funds

- 'Payment service provider' means a natural or legal person (as defined) providing transfer of funds services.
- 'Intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediate payment service provider.

5.2.12 Accordingly, a financial sector business needs to consider which role it is fulfilling when it is involved in a payment chain. For example, a bank or building society effecting an electronic funds transfer on the direct instructions of a customer to the debit of that customer's account will clearly be a PSP whether it undertakes the payment itself (when it must provide its customer's details as the payer), or via an intermediary PSP. In the latter case it must provide the required information on its customer and payee to the intermediary PSP including when it inputs the payment through an electronic banking product supplied by the intermediary PSP.

5.2.13 In other circumstances when a financial sector business, whether independent of the PSP or a specialist function within the same group, passes the transaction through an account in its own name, it may reasonably consider itself under the above definitions as the payer, rather than the PSP, even though the transaction relates ultimately to a customer, e.g., mortgages, documentary credits, insurance claims, financial markets trades. In these cases, if XYZ is the name of the financial sector business initiating the transfer as a customer of the PSP, XYZ can input its own name if using an electronic banking product. There is nothing in the Regulation to prevent including the name of the underlying client elsewhere in the transfer, if XYZ wishes to do so.

5.3 Application of CDD measures

Regulation 28(1)

5.3.1 Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where applicable, beneficial owners. The purpose and intended nature of the business relationship must also be assessed, and if appropriate, information on this obtained.

Identification and verification of the customer

Regulation 28(2)(a)

5.3.2 The firm *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the firm verifying some of this information against documents or information obtained from a reliable source which is independent of the customer.

5.3.3 The term ‘customer’ is not defined in the ML Regulations, and its meaning has to be inferred from the definitions of ‘business relationship’ and ‘occasional transaction’, the context in which it is used in the ML Regulations, and its everyday dictionary meaning. It should be noted that for AML/CTF purposes, a ‘customer’ may be wider than the FCA Glossary definition of ‘customer’.

5.3.4 In general, the customer will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried

out. Where, however, there are several parties to a transaction, not all will necessarily be customers. Further, more specific, guidance for relevant sectors is given in Part II. Section 5.6 is also relevant in this context.

Regulation 4

5.3.5 A "business relationship" is defined in the ML Regulations as a business, professional or commercial relationship between a firm and a customer, which is connected to the business of the firm, and is expected by the firm at the time when contact is established to have an element of duration. A relationship need not involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.

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

5.3.6 An "occasional transaction" for CDD purposes means:

- a transfer of funds within the meaning of article 3.9[1] of the funds transfer regulation exceeding €1,000; or
- a transaction carried out other than in the course of a business relationship (e.g., a single foreign currency transaction, or an isolated instruction to purchase shares), amounting to €15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

5.3.7 The factors linking transactions to assess whether there is a business relationship are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period of time, or where a customer regularly transfers funds to one or more sources. For lower-risk situations that do not otherwise give rise to a business relationship, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

Identification and verification of a beneficial owner

Regulations 6(9),

5.3.8 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted. In respect of private individuals the customer himself is the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement on firms to make proactive searches for beneficial owners in such cases, but they should make appropriate enquiries where it appears that the customer is not acting on his own behalf.

---

[1] 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

(a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012;

(b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012;

(c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border;

(d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

Regulation 5(1),(3)

5.3.9 The ML Regulations define beneficial owners as individuals either 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. See also 5.3.170.

Regulation 6(1)

5.3.10 In relation to a trust, the ML Regulations define the beneficial owner as each of:

- 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;
- any individual who has control over the trust.

Regulation 6(3)

5.3.11 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 5.3.10.

Regulation 6(7),(8)

5.3.12 In relation to a legal entity or legal arrangement which does not fall within 5.3.8-5.3.10, the beneficial owners 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.

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.

5.3.13 Where an individual is required to be *identified* as a beneficial owner in the circumstances outlined in paragraph 5.3.8, where a customer who is a private individual is fronting for another individual who is the beneficial owner, the firm should obtain the same information about that beneficial owner as it would for a customer. For identifying beneficial owners of customers other than private individuals see paragraphs 5.3.126 onwards.

Regulation 28(2)(a),(b), (4)(b),(18)

5.3.14 The *verification* requirements under the ML Regulations are, however, different as between a customer and a beneficial owner. The identity of a customer or beneficial owner must be verified on the basis of documents or information obtained from a reliable source which is independent of the customer. For these purposes, documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the firm by or on behalf of that person. The obligation to verify the identity of a beneficial owner, however, is for the firm to take reasonable measures so that it is satisfied that it knows who the beneficial owner is. It is up to each firm to consider whether it is appropriate, in light of the money laundering or terrorist financing risk associated with the business relationship, to make use of

records of beneficial owners in the public domain, ask their customers for relevant data, require evidence of the beneficial owner's identity on the basis of documents or information obtained from a reliable source which is independent of the customer, or obtain the information in some other way.

5.3.15 In low risk situations, therefore, it may be reasonable for the firm to confirm the beneficial owner's identity based on information supplied by the customer. This could include information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that they are known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the firm.

Regulation 6(1)(c)(d)

5.3.16 In some trusts and similar arrangements, instead of being an individual, the beneficial owner may be a class of persons who may benefit from the trust (see paragraphs 5.3.258ff). Where only a class of persons is required to be identified, it is sufficient for the firm to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class.

Existing customers

Regulations 27(8), 29(7)

5.3.17 Firms must apply CDD measures at appropriate times to its existing customers on a risk-sensitive basis. Firms must also apply CDD measures to any anonymous accounts, ~~or~~ passbooks or anonymous safe-deposit boxes before they are used. The obligation to report suspicions of money laundering, or terrorist financing, however, applies in respect of *all* the firm's customers, as does the UK financial sanctions regime (see paragraphs 5.3.54-5.3.61).

Regulation 27(8)(zb)

Firms must apply CDD measures when they have any legal duty (eg. ML Regulation 28(3A)) to contact an existing customer to review any information relating to the beneficial ownership of the customer.

Firms must also apply CDD measures when they have to contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015 (eg. FATCA, CRS, DAC2).

Firms should consider whether information received as a result of any of these obligations contains changes that require CDD measures to be applied on a risk based approach.

Regulation 27(9)

5.3.18 As risk dictates, therefore, firms must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

5.3.19 Firms that do not seriously address risks (including the risk that they have not confirmed the identity of existing customers) are exposing themselves to the possibility of action for breach of the FCA Rules, or of the ML Regulations.

5.3.20 A firm may hold considerable information in respect of a customer of some years' standing. In some cases the issue may be more one of collating and assessing information already held than approaching customers for more identification data or information.

Acquisition of one financial services firm, or a portfolio of customers, by another

5.3.21 When a firm acquires the business and customers of another firm, either as a whole, or as a portfolio, it is not necessary for the identity of all existing customers to be re-verified, provided that:

- all underlying customer records are acquired with the business; **or**
- a warranty is given by the acquired firm, or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers have been verified.

It is, however, important that the acquiring firm's due diligence enquiries include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired firm (or by the vendor, in relation to a portfolio) have been carried out in accordance with UK requirements.

5.3.22 In the event that:

- the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or
- the procedures cannot be checked; or
- the customer records are not accessible by the acquiring firm,

verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the transferee, in line with the acquiring firm's risk-based approach, and the requirements for existing customers opening new accounts.

Nature and purpose of proposed business relationship

Regulation 28(2)(c) 5.3.23 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard. Whether, and to what extent, the customer has contact or business relationships with other parts of the firm, its business or wider group can also be relevant, especially for higher risk customers. The customer may have different risk profiles in different parts of the business or group.

5.3.24 Depending on the firm's risk assessment of the situation, carried out in accordance with the guidance set out in Chapter 4, information that might be relevant may include some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- the origin of the initial and ongoing source(s) of wealth and funds (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

5.3.25 Having a lower money laundering and/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, in particular for ongoing monitoring of transactions.

5.3.26 When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, firms should take into account risk variables relating to those risk categories, including those set out in the ESA Risk Factor Guidelines[2] (see Annex 4-II). These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting on the appropriate level of CDD measures. Examples of such variables include:

- the purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship

Keeping information up to date

Regulation 28(11)(b)

5.3.27 Documents or information obtained for the purposes of applying CDD measures, held about customers, must be kept up to date. Once the identity of 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, firms must take steps to ensure that they hold appropriate up-to-date information on their customers. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

5.3.28 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.

Characteristics and evidence of identity

[2] These Guidelines were published on 26 June 2017, to take effect by 26 June 2018. See https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

5.3.29 The identity of an individual has a number of principal aspects: i.e., his/her given name (which of course may change), supported by date of birth. Knowledge of an individual's residential address is also central to being reasonably satisfied that the customer is who he says he is, perhaps especially for customers with more common names. Other facts about an individual accumulate over time: e.g., family circumstances and addresses, employment and business career, contacts with the authorities or with other financial sector firms, physical appearance.

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

Evidence of identity

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

5.3.31 The ML Regulations require that customer due diligence must be carried out 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, both at on-boarding stage and subsequently when due diligence is revised/updated.

5.3.32 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 that have dealt with the customer for some time.

Regulation 28(19)

5.3.33 An increasing amount of data on individuals is held electronically/digitally, in various forms, and by various organisations. Evidence of identity can also be obtained by means of a digital identification process, including using an eIDAS electronic identification (eID) means or eIDAS trust service.[3] 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, therefore firms should be satisfied that any process from which such information is obtained 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 that person. Firms should therefore document steps taken in this regard. ~~Electronic databases, however, are becoming ever more sophisticated and widespread, and are likely to be increasingly used; firms should be satisfied that their choice of such sources meets the CDD test of reliability and independence.~~

Regulation 28(12)

5.3.34 How much identity information or evidence to ask for, the balance between asking for documents and using electronic sources, digital identification and/or trust services, and what to verify, in order to be

[3] Regulation 2014/910/EU of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market

reasonably satisfied as to a customer's identity, and to guard against impersonation, are matters for the judgement of the firm, which must be exercised on a risk-based approach, as set out in Chapter 4, taking into account factors such as:

- the nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification);
- the nature and length of any existing or previous relationship between the customer and the firm;
- the nature and extent of any assurances from other regulated firms that may be relied on; and
- whether the customer is physically present.

5.3.35 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

5.3.36 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, without any such checks being carried out. There is a broad hierarchy of documents:

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

5.3.37 In their procedures, therefore, firms will in many situations need to be prepared to accept a range of documents.

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

Electronic evidence

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

5.3.40 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.

5.3.41 Firms 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.

5.3.42 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 firm 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. Where the user is required to give their approval, consideration should be given to the possibility that the user may prevent certain information being accessed to conceal certain facts.

5.3.43 Given the increasing prevalence of social media data, firms may consider it appropriate, in some circumstances, to take such information into account as corroboration for, or supplementary to, their CDD measures. However, firms should have regard to the risks inherent in the reliability of this data, as well have regard to using such information responsibly under privacy and data protection laws. ~~.~~

5.3.44 In using an electronic source or digital identity or trust service ~~source~~ to verify a customer's identity, firms should ensure that they are able to demonstrate that they have both verified that the customer (or beneficial owner) exists, and satisfied themselves that the applicant seeking the business relationship 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 or a trust service that incontrovertibly link the potential customer (or beneficial owner) to the electronic/digital identity information.

5.3.45 Firms 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, firms 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

5.3.46 A number of commercial organisations which access many data sources are accessible online by firms, and may provide firms with 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 PEPs or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

5.3.47 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 assurance or scored levels of verification~~authentication~~ that are established through the accumulation of specific pieces of identity information.

5.3.48 Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others where no such proof is required. 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 firm under its risk-based approach~~.

5.3.49 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 in line with the firm's risk based approach.

5.3.50 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, or be done through an organisation which meets the criteria in paragraphs 5.3.51-5.3.52. 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, although it may be sufficient, where, for example, the source has been issued by a government authority and contains cryptographic security features.

Criteria for use of a provider of electronic verification of identity, digital identity or trust service

5.3.51 Some commercial organisations providing digital identities, electronic or ~~/~~digital identity verification, or trust services are free-standing and set their own operating criteria, whilst others may be part of an association or arrangement which, in order to admit organisations to 'membership' require them to demonstrate that they meet certain published criteria – for example, in relation to data sources used, or recency of information - and carry out some form of checks on continuing compliance.

Regulation 28(19)

5.3.52 Before using an ~~commercial~~ organisation for digital identities, electronic or digital identity verification~~ of identity~~, firms should be satisfied that information supplied by the ~~data~~ provider is considered to be sufficiently extensive, reliable, ~~and~~ accurate, ~~and~~ independent of the customer, and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. This judgement may be assisted by considering whether the ~~identity~~ provider meets the following criteria:

- it is a notified identity scheme under the eIDAS Regulation[4];
- it is provided by means of a trust service covered by the eIDAS Regulation[5]; or
- it provides a service as defined by eIDAS regulation or has a similar level of assurance as eIDAS notified schemes;
- it is recognised, through registration with the Information Commissioner's Office (or national equivalent for EEA/EU registered organisations), 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 or~~,~~ 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 firm 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.
- it keeps sufficient records of information used to provide its services.

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

Persons firms should not accept as customers

Persons and entities subject to financial sanctions

5.3.54 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. A Consolidated List of all targets to whom financial sanctions apply is maintained by OFSI, and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at:

[4] https://eceuropa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+prenotified+and+notified+eID+schemes+under+eIDAS

[5] https://webgate.ec.europa.eu/tl-browser/#/

www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

5.3.55 The obligations under the UK financial sanctions regime apply to all firms, 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. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although a firm 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 firms to whom this guidance applies, therefore, whether or not they are FCA-regulated or subject to the ML Regulations, 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.

5.3.56 The origins of such sanctions and the sources of information for the Consolidated List are set out in Part III, section 4.

5.3.57 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

5.3.58 To reduce the risk of breaching obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets, or their agents. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and then have appropriate regard to other parties involved.

5.3.59 Firms need to have some means of monitoring payment instructions to ensure that proposed payments to targets or their agents are not made. The majority of payments made by many firms will, however, be to other regulated firms, rather than to individuals or entities that may be targets.

5.3.60 Where a firm freezes funds under financial sanctions legislation, or where it 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 6.33 to 6.42.

CTA 2008, Schedule 7

5.3.61 Under certain circumstances, HM Treasury may issue directions to a firm in relation to customer due diligence; ongoing monitoring; systematic reporting; and limiting or ceasing business. Details of any such HM

Treasury directions will be found at www.hm-treasury.gov.uk. Guidance on complying with directions issued by HM Treasury under CTA 2008, Schedule 7 is given in Part III, section 5.

5.3.62 Trade sanctions can be imposed by governments or other international authorities, and these can have financial implications. Where the proposed trade deal also involves a person or entity which is subject to an asset freeze, a firm will need a licence from OFSI to deal with the funds or economic resources of the designated individual, as well as the export licence from the Department for International Trade. Firms 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 firm's procedures. Further information and links to lists of affected countries can be found at: https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions.

Illegal immigrants

s40 (1), (2) 5.3.63 Under the Immigration Act 2014, a bank or building society must not open a current account for a person who is in the UK but does not have leave to enter or remain in the UK. These immigration checks must also be carried out on existing personal current accounts on a quarterly basis and Home Office notified of a disqualified person's account or application for an account.[6]

s 40 (3) 5.3.64 Confirmation that a person is not entitled to enter or remain in the UK can be obtained through carrying out a check with a specified[7] anti-fraud organisation or a specified data matching authority.

5.3.65 Normal CDD measures must still be applied to the customer once his immigration status has been checked. Where a current account is refused, the person must be informed it is for reasons of immigration status.

Shell banks and anonymous accounts

Regulation 34 (2), (3), (4)(b) 5.3.66 Firms must not enter into, or continue, a correspondent relationship with a shell bank. Firms must take appropriate measures to ensure that it does not enter into or continue a correspondent relationship with a bank that is known to allow its accounts to be used by a shell bank. A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate.

Regulation 29(6),(7) 5.3.67 Firms carrying on business in the UK must not set up an anonymous account, ~~or~~ an anonymous passbook, or an anonymous safe-deposit box for any new or existing customer. All firms carrying on business in the UK must apply CDD measures to all existing anonymous accounts, ~~and~~ passbooks and safe-deposit boxes before such accounts, ~~or~~ passbooks or safe-deposit boxes are used in any way.

[6] See The Immigration Act 2015 (Current Accounts)(Compliance &c) Regulations 2016 s2

[7] See The Immigration Act 2014 (Specified Anti-fraud Organisation) Order 2014 SI 2014/1798

5.3.68 Firms should pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that may favour anonymity and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

Private individuals

General

5.3.69 Paragraphs 5.3.71 to 5.3.91 refer to the standard identification requirement for customers who are private individuals; paragraphs 5.3.92 to 5.3.125 provide further guidance on steps that may be applied as part of a risk-based approach.

5.3.70 Depending on the circumstances relating to the customer, the product and the nature and purpose of the proposed relationship, firms may also need to apply the following guidance to identifying, and verifying the identity of, beneficial owners, and to other relevant individuals associated with the relationship or transaction (but see paragraphs 5.3.8 to 5.3.16).

Obtain standard evidence

Identification

5.3.71 The firm should obtain the following information in relation to the private individual:

- full name
- residential address
- date of birth

Verification

Regulation 28(18)(b) 5.3.72 Verification of the information obtained must be based on reliable sources, independent of the customer – which might either be a document or documents produced by the customer, or electronically by the firm, 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 firm by the customer. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification. Customers should be discouraged from sending original valuable documents by post.

A – DOCUMENTARY EVIDENCE

5.3.73 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 that has~~, 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 firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

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

5.3.75 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 FCA-regulated firm in the UK financial services sector, 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
- Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant
- Instrument of a court appointment (such as liquidator, or grant of probate)
- Current council tax demand letter, or statement

5.3.76 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 5.3.45). Consideration should be given to an increased risk of forgery or counterfeiting of paper documents as customer statements can potentially be indistinguishable from originals. Where a member of the firm'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).

5.3.77 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[8]) should enable most individuals to meet the identification requirement for AML/CTF purposes. The firm'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. For customers who cannot provide the standard evidence, other documents may be appropriate (see paragraphs 5.3.108 to 5.3.125).

5.3.78 Some consideration should be given as to whether the documents relied upon are forgeries or counterfeits~~d~~. 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. Examples of sources of information include CIFAS, the Fraud Advisory Panel and the Serious Fraud Office. 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.

B – ELECTRONIC EVIDENCE AND DIGITAL IDENTITY

5.3.79 When using an electronic ~~/digital~~ source or digital identity to verify a customer's identity, firms 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 is, in fact, that customer (or beneficial owner).

5.3.80 Electronic verification may be carried out by the firm either direct, using as its basis the customer's full name, address and date of birth, or through an organisation which has been considered per~~meets~~ the criteria in paragraphs 5.3.51 and 5.3.52.

5.3.81 For verification purposes, a firm may approach an electronic source, digital identity or trust provider~~/digital sour~~ce of its own choosing, or the potential customer may elect to offer the firm 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 5.3.51 and 5.3.52.

5.3.82 Some digital identity, electronic sources or trust service providers focus on using primary identity documents, sometimes using biometric

[8] 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.

data. Others electronic sources accumulate corroborative information which in principle is separately available elsewhere. Some sources areinformation is independent of the customer, whilst others is are under their 'control' in the sense that their approval is required for information to be included.

5.3.83 As well as requiring an commercial organisation used for electronic verification to or digital identity to be considered permeet the criteria set out in paragraphs 5.3.51 and 5.3.52, it is important that the process of electronic verification meets an appropriate level of assuranceconfirmation before it can be judged to satisfy the firm's legal obligation.

5.3.84 Commercial organisations that provide electronic verification of identity or digital 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 assurance or scored level of verificationauthentification has been reached. Firms 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 5.3.46-5.3.50, and cumulatively meet an appropriate level of confirmation in relation to the risk assessed in the relationship.

C – MITIGATION OF IMPERSONATION RISK

5.3.85 Whilst some types of financial transaction have traditionally been conducted on a non-face-to-face basis, other types of transaction and relationships are increasingly undertaken in this way: e.g., internet and telephone banking, online share dealing.

5.3.86 Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non face-to-face business, such as applications submitted by post, 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 applications without incurring extra cost or the risk of detection;
- the absence of physical documents; and
- the speed of electronic transactions.

5.3.87 The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in itself increase the risk attaching to the transaction or activity. A firm should take account of such cases in developing their systems and procedures.

5.3.88 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.

5.3.89 Where identity is verified electronically, copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms 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, digital signing by a qualified trust service certificate or other secret data may be set up within the ~~electronic/digital~~ identity, or may be supplied to a verified mobile phone, or through a verified bank account, on a one-time basis, or
- following the guidance in paragraph 5.3.90.

5.3.90 The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction;
- verifying additional aspects of the customer's identity (see paragraph 5.3.29);
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);
- internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other secure authentication means~~passwor~~ which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;
- other card or account activation procedures;

- requiring copy documents to be certified by an appropriate person.

5.3.91 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

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

5.3.93 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.

5.3.94 For higher risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see sections 5.5 and 5.7).

Executors and personal representatives

Regulation 6(6)

5.3.95 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[9].

In circumstances where an account is opened or taken over by executors or administrators for the purpose of winding up the estate of a deceased person, firms 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.

5.3.96 When a customer's account is taken over by their personal representatives, firms may find the Framework for authorising people wanting to operate a

[9] 1900 c.55. Sections 6 and 7 were amended by the Succession (Scotland) Act 1964 (c.41)

bank account for someone else'[10] agreed between the Office of the Public Guardian, BBA, Building Societies Association, the Law Society in England and Wales and others a useful source of practical advice.

Court of Protection orders and court-appointed deputies

2005, c 9
SI 2007/1253

5.3.97 Under the Mental Capacity Act 2005 (and related Regulations), the Court of Protection will be able to make an order concerning a single decision in cases where a one-off decision is required regarding someone who lacks capacity. The Court can also appoint a deputy or deputies (previously referred to as receivers) where it is satisfied that a series of decisions needs to be made for a person who lacks capacity.

5.3.98 Firms may accept the court documents appointing the deputy, or concerning a single act, as evidence of authority~~identity~~ of the person appointed.

Attorneys

5.3.99 When a person deals with assets under a power of attorney, that person is also a customer of the firm. Consequently, the identity of holders of powers of attorney should be verified, in addition to that of the donor. In the case of a joint and several power of attorney, the identity of the person acting separately may be verified on its own, without the need to verify the identity of all persons when they are not acting jointly.

5.3.100 Other than where the donor or grantor of a power of attorney is an existing customer of the firm, his identity must be verified. In many cases, these customers may not possess the standard identity documents referred to in paragraphs 5.3.75ff, and firms may have to accept some of the documents referred to in paragraph 5.3.115. 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, severe loss of mental capacity); due consideration should be given to the individual's circumstances in such cases.

5.3.101 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 firm 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 firm will not necessarily know whether or not the donor has lost capacity.

Source of funds as evidence

5.3.102 Under certain conditions, where the money laundering or terrorist financing risk in a product is considered to be at its lowest, a payment drawn on an account with a UK or EU regulated credit institution, or with one from an assessed low risk jurisdiction, and which is in the sole or joint name of the customer, may satisfy the standard identification requirement. Whilst the payment may be made between accounts with regulated firms or by cheque or debit card, the accepting firm must be able to confirm that

[10] http://www.mentalhealthlaw.co.uk/media/Banking_guidance_for_banks_3-4-13.pdf

the payment (by whatever method) is from a bank or building society account in the sole or joint name(s) of the customer. Part II, sector 7: *Life assurance, and life-related pensions and investment products*, has an exception to this in respect of direct debits.

5.3.103 Whilst it is immaterial whether the transaction is effected remotely or face-to-face, each type of relationship or transaction that is entered into must be considered before determining that it is appropriate to rely on this method of verification. Firms will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance. Part II, sector 3: *Electronic Money* includes guidance on accepting the funding instrument used to load a purse as a form of initial verification in low risk situations, subject to compensating monitoring controls and turnover limits, and establishing that the customer has rightful control over the instrument.

5.3.104 One of the restrictions that will apply to a product that qualifies for using the source of funds as evidence will be an inability to make payments direct to, or to receive payments direct from, third parties. If, subsequent to using the source of funds to verify the customer's identity, the firm decides to allow such a payment or receipt to proceed, it should verify the identity of the third party. A further restriction would be that cash withdrawals should not be permitted, other than by the customers themselves, on a face-to-face basis where identity can be confirmed.

5.3.105 If a firm proposing to rely on the source of funds has reasonable grounds for believing that the identity of the customer has not been verified by the firm on which the payment has been drawn, it should not permit the source of funds to be used as evidence, and should verify the customer's identity in line with the appropriate standard requirement.

5.3.106 If a firm has reason to suspect the motives behind a particular transaction, or believes that the business is being structured to avoid the standard identification requirement, it should not permit the use of the source of funds as evidence to identify the customer.

5.3.107 Part II, sector 8: *Non-life providers of investment fund products* provides additional guidance to investment fund managers in respect of customers whose identity may not need to be verified until the time of redemption.

Customers who cannot provide the standard evidence

5.3.108 Some customers may not be able to produce identification information equivalent to the standard. Such cases may include, for example, some low-income customers in rented accommodation, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependant spouses/partners or minors, students, refugees and asylum seekers, migrant workers and prisoners. The firm will therefore need an approach that compensates for the difficulties that such customers may face in providing the standard evidence of identity.

SYSC 6.3.7 (5) G
Financial Inclusion Task Force, December 2010

5.3.109 The FCA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. The term is sometimes used in a narrower sense, for

example, the Financial Inclusion Task Force refers to those who, for specific reasons, do not have access to mainstream banking or financial services - that is, those at the lower end of income distribution who are socially/financially disadvantaged and in receipt of benefits, or those who chose not to seek access to financial products because they believed that they will be refused.

5.3.110 Firms offering financial services directed at the financially aware may wish to consider whether any apparent inability to produce standard levels of identification evidence is consistent with the targeted market for these products.

5.3.111 As a first step, before concluding that a customer cannot produce evidence of identity, firms will have established that the guidance on initial identity checks for private individuals set out in paragraphs 5.3.71 to 5.3.107 cannot reasonably be applied in view of the circumstances of the relevant customer.

5.3.112 The guidance at paragraph 5.3.75 does not require that in all cases a customer's address should be verified – the standard verification is verification of name and a choice between verifying address or date of birth. Providing the standard evidence of address can be a particular difficulty for many new arrivals to the UK, and firms should have regard to this fact in deciding whether, in particular cases, to insist on address verification, and if so, how this might be satisfied.

5.3.113 Guidance on verifying the identity of most categories of customers who cannot provide the standard evidence is given in Part II, sector 1: *Retail banking*. Guidance on cases with more general application is given in paragraphs 5.3.115 to 5.3.125.

5.3.114 Where a firm concludes that an individual customer cannot reasonably meet the standard identification requirement, and that the provisions in Part II, sector 1: *Retail banking*, Annex 1-I, cannot be met, it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he says he is.

Persons without standard documents, in care homes, or in receipt of pension

5.3.115 An entitlement letter from the DWP, or a letter from the DWP confirming that the person is in receipt of a pension, could provide evidence of identity. If this is not available, or is inappropriate, a letter from an appropriate person, for example, the matron of a care home, may provide the necessary evidence.

Those without the capacity to manage their financial affairs

5.3.116 Guidance on dealing with customers who lack, or are losing, capacity to manage their affairs, covering Powers of Attorney; Court of Protection Orders; and Appointeeship, are set out in a BBA leaflet, "Guidance for people wanting to manage a bank account for someone else", which can be obtained from the British Bankers' Association at www.bba.org.uk. (see also paragraphs 5.3.97 – 5.3.101). Although this leaflet is directed at banks, its contents have more general application.

Gender reassignment

5.3.117 A firm should satisfy itself (for example, on the basis of documentary medical evidence) that the gender transfer of a customer is genuine (as with a change of name). Such cases usually involve transferring a credit history to a reassigned gender. This involves data protection, not money laundering issues. The consent of the person involved is necessary.

Students and young people

5.3.118 When opening accounts for students or other young people, the standard identification requirement should be followed as far as possible (see paragraphs 5.3.71 – 5.3.107). In practice, it is likely that many students, and other young people, will have a passport, and possibly a driving licence. Where the standard requirement would not be relevant, however, or where the customer cannot satisfactorily meet this, other evidence could be obtained by obtaining appropriate confirmation(s) from the applicant's workplace, school, college, university or care institution (see UK Border Agency website http://www.bia.homeoffice.gov.uk/employers/points/ and Part II, sector 1: *Retail banking*, Annex 1-I). Any confirmatory letter should be on appropriately headed notepaper; in assessing the strength of such confirmation, firms should have regard to the period of existence of the educational or other institution involved, and whether it is subject to some form of regulatory oversight. UCAS also maintain a database of students who have confirmed places at a University/Higher Education establishment, which is accessible on subscription (see www.ucasmedia.com/).

5.3.119 All international students, other than those from EEA countries or Switzerland, undergo rigorous checks by the immigration services at home and abroad in order to be satisfied as to their identity and bona fides before they are given leave to enter or remain in the UK as a student or prospective student. Applicants must meet the requirements of the Student Immigration Rules and must provide documentation which demonstrates that they intend to study, and have been accepted, on a course of study at a bona fide institution. This includes the provision of a course admission letter from the education institution. If they cannot provide the documents they will not be given leave to enter or remain in the UK.

5.3.120 Often, a business relationship in respect of a minor will be established by a family member or guardian. In cases where the adult opening the account or establishing the relationship does not already have an existing relationship with the firm, the identity of that adult should be verified and, in addition, the firm should see one of the following documents (or similar documents issued in other jurisdictions) in the name of the child:

- birth certificate
- passport
- NHS Medical Card
- Child benefit documentation
- Child Tax Credit documentation
- National Insurance Card (for those aged 16 and over)

Financially excluded

5.3.121 Further guidance on verifying the identity of financially excluded persons is given in Part II, sector 1: *Retail banking*, paragraphs 1.38 – 1.41. A proportionate and risk-based approach will be needed to determine whether the evidence available gives reasonable confidence as to the identity of a customer.

5.3.122 Where a firm has concluded that it should treat a customer as financially excluded for the purposes of customer identification, and the customer is identified by means other than standard evidence, the reasons for doing so should be documented.

5.3.123 The "financially excluded" are not a homogeneous category of uniform risk, and firms should consider the risk presented in any particular case. Some financially excluded persons may represent a higher risk of money laundering regardless of whether they provide standard or non-standard tokens to confirm their identity, e.g., a passport holder who qualifies only for a basic account on credit grounds. Firms may wish to consider whether enhanced due diligence (see section 5.5) or monitoring (see section 5.7) of the size and expected volume of transactions would be useful in respect of some financially excluded categories, based on the firm's own experience of their operation.

5.3.124 In other cases, where the available evidence of identity is limited, and the firm judges that the individual cannot reasonably be expected to provide more, but that the business relationship should nevertheless go ahead, it should consider instituting enhanced monitoring arrangements over the customer's transactions and activity (see section 5.7). In addition, the firm should consider whether restrictions should be placed on the customer's ability to migrate to other, higher risk products or services.

5.3.125 Where an applicant produces non-standard or incomplete documentation, staff should not cite the ML Regulations (or other regulation relating to the prevention of money laundering and/or terrorist financing) as an excuse for not opening an account without giving proper consideration to the evidence available, referring up the line for advice as necessary. It may be that at the conclusion of that process a considered judgement may properly be made that the evidence available does not provide a sufficient level of confidence that the applicant is who he claims to be, in which event a decision not to open the account would be fully justified. Firms should bear in mind that the ML Regulations are not explicit as to what is and is not acceptable evidence of identity.

Customers other than private individuals

5.3.126 Depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into in the customer's own name, or in that of specific individuals or other entities on its behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

Regulation 28(3A)

Where the customer is a legal person, company, trust, foundation, or similar legal arrangement, reasonable measures must be taken to understand the ownership and control structure of the entity.

Regulation 28(4)

5.3.127 In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm's objective must be to know who has ownership or control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) will be carried out on a risk-based approach, following the guidance in paragraphs 5.3.8 to 5.3.16, and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

5.3.128 Firms also have obligations under the UK financial sanctions regime (see Part III, section 4: *Compliance with the UK financial sanctions regime)* which require the collection of information in relation to trustees, directors or equivalent (see Part III, paragraphs 4.83 – 4.85). In determining the information to be collected, therefore, firms should take account of their information needs in relation to sanctions compliance.

5.3.129 Certain other information about the entity should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer/product/delivery channel combination, a firm should decide the extent to which the identity of the entity should be verified. The firm should also decide what additional information in respect of the entity and, potentially, some of the individuals behind it, should be obtained (see section 5.5).

Regulation 30A(1)

5.3.129A Firms must obtain proof of registration or an excerpt of the register of the company, unregistered company, the limited liability partnership as the case may be, or the registrar in the case of an eligible Scottish partnership, before establishing a business relationship (with UK entities). The information required relates to persons of significant control (PSC) as per the PSC registers and may be obtained from the customer, Companies House, or a third party provider.

If the firm finds a discrepancy between information relating to the beneficial ownership of the company which it collects as above, and information which becomes available to it whilst carrying out its duties under the ML Regulations (during its onboarding process), the discrepancy must be reported to Companies House.

Beneficial ownership in this context means a person of significant control (PSC) per the information held in the PSC register and not as defined in the ML Regulations. Information on the PSC register may thus differ from other beneficial ownership information and not necessarily be inaccurate.

Discrepancies should be material to be reportable. For example, a material discrepancy would arise when there is a missing or different person (legal or natural) recorded, as compared between information in the PSC register and information obtained at onboarding. The material discrepancy report

should be made as soon as reasonably possible when discovered. A discrepancy itself does not prohibit the onboarding of a customer – the nature and relevance of the discrepancy may be assessed by firms with their CDD process and risk based approach during onboarding, and considering whether there are reasonable grounds for suspicion. A discrepancy report is not a substitute for a suspicious transaction report (SAR) and the requirement to submit a SAR where appropriate remains. Firms are not required to check for or report discrepancies involving existing customers.

For further information (including what Companies House could constitute as a material discrepancy) see: https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity#when-to-make-a-discrepancy-report

Regulation 27(9)(c) and 33(1)(g)

5.3.130 Where an entity is known to be linked to a PEP (as a result of the PEP being a beneficial owner of the entity), or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher risk category, and that enhanced due diligence measures should therefore be applied (see sections 5.5 and 5.7).

5.3.131 Many entities, both in the UK and elsewhere, operate internet websites, which contain information about the entity. Firms should bear in mind that this information, although helpful in providing much of the material that a firm might need in relation to the company, its directors and business, is not independently verified before being made publicly available in this way.

5.3.132 This section provides guidance on verifying the identity of a range of non-personal entities, as follows:

- Regulated financial services firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.133 to 5.3.138)
- Other firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.139 to 5.3.142)
- Corporate customers (other than regulated firms) (paragraphs 5.3.143 to 5.3.176)
- Partnerships and unincorporated businesses (paragraphs 5.3.177 to 5.3.191)
- Public sector bodies, governments, state-owned companies and supranationals (paragraphs 5.3.192 to 5.3.203)
- Sovereign Wealth Funds (paragraphs 5.3.204-5.3.227)
- Pension schemes (paragraphs 5.3.228 to 5.3.237)
- Charities, church bodies and places of worship (paragraphs 5.3.238 to 5.3.257)
- Other trusts and foundations (paragraphs 5.3.258 to 5.3.282)
- Clubs and societies (paragraphs 5.3.283 to 5.3.293)

Regulated financial services firms subject to the ML Regulations (or equivalent)

Regulation 37(3)(a)

5.3.133 In determining whether a business relationship presents a low degree of risk of ML/TF, and therefore the extent to which it is appropriate to apply SDD measures, a firm must take into account, inter alia, whether the

customer is a credit institution or a financial institution which is subject to the requirements in the ML Regulations.~~fourth money laundering directive.~~

Regulation 37(3)

5.3.134 In their determination of the low degree of ~~low~~ risk, firms must also take into account whether the country where the customer is resident, established or registered, or in which it operates, is an EEA state or an assessed low risk jurisdiction.

Regulation 37(1)

5.3.135 If the firm determines that the situation in relation to another regulated financial services firm presents a low degree of ML/TF risk, simplified due diligence may be applied (see section 5.4).

5.3.136 When applying SDD measures firms must continue to comply with the requirements of Regulation 28 of the ML Regulations although the extent, timing or type of measures undertaken may be adjusted to reflect its determination per 5.3.135.~~Applying simplified due diligence might involve:~~

~~➢ checking with the home country central bank or relevant supervisory body; or~~
~~➢ checking with another office, subsidiary, branch or correspondent bank in the same country; or~~
~~➢ checking with a regulated correspondent bank of the overseas institution; or~~
~~➢ obtaining from the relevant institution evidence of its licence or authorisation to conduct financial and/or banking business.~~

5.3.137 Firms should:

- ~~-~~record the steps they have taken to check the status of the other regulated firm.
- take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer
- document the rationale for the decision to apply SDD.

5.3.138 Firms must continue to monitor business relationships and transactions to detect unusual or suspicious transactions.~~Firms should take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer.~~

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

5.3.139 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 as a financial services business, 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 5.3.163 to 5.3.176; 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 example, as trustees, their identity should normally be verified as for any other private individual.

5.3.140 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.141 Some consideration should be given as to whether documents relied upon are forgeries or counterfeits~~d~~. 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.

Regulation 37(5)(6)

5.3.142 Firms that are subject to the ML Regulations, and, which hold client money in pooled accounts (whether in a bank account or through a securities holding), are in principle obliged to verify the identities of their clients. Financial services firms with which such client accounts are held are, however, permitted to apply SDD measures to the holders of such funds, provided that:

- the business relationship with the holder of the pooled account presents a low risk of ML/TF;
- the information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the firm;
- if the holder of the pooled account is in another EEA state, the holder is subject to the requirements in national legislation implementing the fourth money laundering directive, and is supervised for compliance with these requirements.

As a practical matter, firms may reasonably apply a similar approach to such client accounts which only contain the funds of a single beneficial owner. Firms should also be satisfied that the customer applies robust and risk-sensitive CDD measures to their own clients and their clients' beneficial owners. It may be appropriate for firms to take risk-sensitive measures to assess the adequacy of its customer's CDD policies and procedures, for example by liaising directly with the customer or by sample-testing the customer's ability to provide CDD information upon request.

Corporate customers (other than regulated firms)

5.3.143 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, firms should take account of the availability of public information in respect of different types of company.

Regulation 432

5.3.144 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 or has an existinga business relationship with a firm, where the firm is required to apply CDD measures, the corporate must on request provide the firm with:

- information identifying
  - its name, registered number, registered office and principal place of business;
  - its board of directors or members of the equivalent management body if no board
  - its senior management
  - the law to which it is subject
  - its legal and beneficial owners;
- its articles of association or other governing documents.

UK body corporates must inform the firm with which they have a business relationship of any change to the above information within 14 days of becoming aware of the change.

These requirements do not apply to corporates as defined per 5.3.156.

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.

5.3.145 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)

5.3.146 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. Firms 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. (More specific guidance on beneficial ownership is given in Part II, Sector 13: *Private equity*, paragraphs 13.49-13.52, which may be of more general interest.)

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

5.3.147 To the extent consistent with the risk assessment carried out in accordance with the guidance in Chapter 4, the firm 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 the product or service.

Regulation 5(1)

5.3.148 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, firms 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
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

5.3.149 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.

5.3.150 Paragraphs 5.3.151 – 5.3.154 refer to the standard evidence for corporate customers, and paragraphs 5.3.155 – 5.3.162 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

Regulation 28(3)(a)

5.3.151 The firm must obtain and verify the following information in relation to the corporate concerned:

- full name
- registered number
- registered office 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 30A

Firms must obtain proof of registration or an excerpt of the register of the corporate before establishing a business relationship.

Regulation 28(3)

5.3.152 The firm 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 firm should verify the information set out in paragraph 5.3.151, 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

5.3.153 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.154 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)

5.3.155 Corporate customers whose securities are admitted to trading on a regulated market in an EEA state or a regulated financial market outside of the EEA whose securities are admitted to equivalent trading disclosure obligations ~~one in an assessed low risk jurisdiction are publicly owned and~~ are generally accountable.

Regulation 28(5)

5.3.156 Where the firm 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 5.3.152 (a)-(c) does not apply (see section 5.4).

Regulation 3(1)

5.3.157 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)

5.3.158 If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. Firms 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 5.3.157, the standard verification requirement for private and unlisted companies should be applied.

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

Other publicly listed or quoted companies

5.3.160 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, firms 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 customer risk, including whether SDD may be applied (see Part III 3.3).~~the level of checks required and the extent to which the customer should be treated as a private company (see paragraphs 5.3.163 - 5.3.176).~~

5.3.161 Firms should note that AIM is not a regulated market under MiFID. However, due diligence requirements at admission and ongoing disclosure requirements on AIM are broadly similar to those of regulated markets. A firm may, therefore, under its risk-based approach, regard the due diligence process for admission to AIM as giving equivalent comfort as to the identity of the company under consideration.

5.3.162 In applying the risk based approach, firms 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 firm 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

5.3.163 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 firms 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)

5.3.164 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 firm's obligations. Where a higher risk of money laundering is associated with the business relationship, however, EDD (and enhanced monitoring) must be applied.

5.3.165 In the UK, a company registry search (or enquiry of the Charities Commission in the case of a Charitable Incorporated Organisation) 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, firms should make similar search enquiries of the registry in the country of incorporation of the applicant for business.

5.3.166 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.

5.3.167 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms 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). A visit to the place of business may be helpful to confirm the existence and activities of the entity.

5.3.168 Firms may find the sectoral guidance in Part II helpful in understanding some of the business relationships that may exist between the customer and other entities in particular business areas.

Directors

5.3.169 Following the firm's assessment of the money laundering or terrorist financing risk presented by the company, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals (paragraphs 5.3.71 to 5.3.125). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other directors. Firms may, of course, already be required to identify 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 5.3.148).

Beneficial owners

Regulation 5
Regulation 28(4),(9)
Regulation 28(3A); 28(8)(b)

5.3.170 As part of the standard evidence, the firm will 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. This forms part of their understanding of the ownership and control structure of the entity. If there is an obligation to identify, but no beneficial owner has been identified, or the firm is not satisfied that the individual identified is the beneficial owner, t~~T~~he firm must take reasonable measures to verify the identity of the senior person in the body corporate responsible for managing it~~those individuals~~ (see also paragraphs 5.3.8 to 5.3.16), and record all actions in doing so, as well as difficulties encountered, where applicable. Firms do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a PSC register.

Where there is no reasonable expectation of certain corporate customers, such as supranational organisations, wholly state-owned entities, certain multilateral financial institutions, government agencies and sovereign wealth funds, having a beneficial owner, firms do not need to verify the identity of the senior person but must nevertheless document the steps taken and record the rationale for their conclusions.

Signatories

5.3.171 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Other considerations

5.3.172 Unless their customer's securities are admitted to trading in a regulated market in an EEA state, firms are required to verify the identity of beneficial owners of corporate customers that are subject to statutory licensing and regulation of their industry (for example, energy, telecommunications) . Under its risk-based approach, however, a firm may feel that, provided that it is confirmed by a reliable source, independent of the customer, imposition of regulatory obligations on such a firm gives an equivalent level of confidence in the company's public accountability. Therefore, evidence that the corporate customer is subject to the licensing and prudential regulatory regime of a statutory regulator in the EU (e.g., OFGEM, OFWAT, OFCOM or an EU equivalent), should satisfy the firm's obligation to verify the identity of such a customer.

Regulation 33(1)(g)

5.3.173 The standard evidence is likely to be sufficient for most corporate customers. If, however, the customer, or the product or delivery channel, 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 product features available – the firm must, on a risk-sensitive basis, apply EDD measures. For example, the firm will need to decide whether it should require additional identity information to be provided and/or verified (see sections 5.6 and 5.7).

5.3.174 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

5.3.175 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. Firms 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.

5.3.176 As a minimum, these procedures should require a firm to obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the firm if the shares are transferred to another party. Depending on its risk assessment of the client, the firm 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 firm will be notified of any changes to records relating to these shares and the custodian.

Partnerships and unincorporated bodies

5.3.177 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) 5.3.178 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, firms should use judgement in determining whether an individual owning or controlling a lower percentage exercises effective control.

Obtain standard evidence

5.3.179 The firm should obtain the following standard evidence in relation to the partnership or unincorporated association:

- full name
- business address
- 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

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

5.3.181 The firm'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.

5.3.182 As part of the standard evidence, the firm will 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 firm must take reasonable measures to verify the identity of those individuals (see paragraphs 5.3.8 to 5.3.16).

5.3.183 Intentionally left blank.

5.3.184 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.

5.3.185 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.186 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

5.3.187 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.

5.3.188 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.3.102 to 5.3.106 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.189 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms 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.

5.3.190 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

5.3.191 Following its assessment of the money laundering or terrorist financing risk presented by the entity, the firm may decide to verify the identity of one or more of the partners/owners as customers. In that event, verification requirements are likely to be appropriate for partners/owners who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets; other partners/owners must be verified as beneficial owners, following the guidance in paragraphs 5.3.8 to 5.3.16.

Public sector bodies, governments, state-owned companies and supranationals (other than sovereign wealth funds)

Regulation 37(3)

5.3.192 In respect of customers which are UK or overseas governments (based in jurisdictions that the firm has determined as low risk), (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the customer, reflecting the firm's determination of the level of ML/TF risk presented. Where the firm determines that the business relationship presents a low degree of risk of ML/TF, SDD measures may be applied. Public sector bodies include state supported schools, colleges, universities and NHS trusts.

5.3.193 Bodies engaged in public administration are different from state-owned bodies which conduct business. The nature of the business relationship established with firms in the financial sector will therefore differ. Public administration involves a different revenue/payment stream from that of most businesses, and may be funded from government sources, or from some other form of public revenues. State-owned businesses, on the other hand, may engage in a wide range of activities, some of which might involve higher risk factors, leading to a different level of CDD being

appropriate. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.

Obtain standard evidence

5.3.194 Firms should obtain the following information about customers who are public sector bodies, governments, state-owned companies and supranationals:

- Full name of the entity
- Nature and status of the entity (e.g., overseas government, treaty organisation)
- Address of the entity
- Name of the home state authority
- Names of directors (or equivalent)

5.3.195 Firms should take appropriate steps to understand the ownership of the customer, and the nature of its relationship with its home state authority.

5.3.196 Firms should, where appropriate, verify the identities of the directors (or equivalent) who have authority to give the firm instructions concerning the use or transfer of funds or assets.

5.3.197 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Signatories

5.3.198 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Schools, colleges and universities

5.3.199 State supported schools, colleges and universities should be treated as public sector bodies, in accordance with the guidance set out in paragraphs 5.3.192 to 5.3.198. The UK Border Agency maintains a register of sponsors www.bia.homeoffice.gov.uk/employers/points/ which may assist firms in verifying the existence of such customers. The register of sponsors lists all organisations that the UK Border Agency has approved to employ migrants or sponsor migrant students.

5.3.200 For independent schools and colleges, firms should refer to the guidance given at paragraph 5.3.253.

Other considerations

5.3.201 The firm's assessment of the money laundering or terrorist financing risk presented by such customers should aim to identify higher risk countries or jurisdictions.

5.3.202 The guidance in paragraphs 5.3.192 to 5.3.200 should be applied to overseas entities, as appropriate to the firm's assessment of the risk that such entities present.

5.3.203 Many governmental, supranational and state-owned organisations will be managed and controlled by individuals who may qualify as PEPs (see paragraphs 5.5.13 to 5.5.23). Firms need to be aware of the increased likelihood of the existence of such individuals in the case of such customers, and deal with them appropriately, having regard to the extent of any risk that the funds of such entities may be used for improper purposes.

Sovereign wealth funds

5.3.204 Sovereign Wealth Funds (SWFs) are defined[11] as special purpose investment funds or arrangements, owned by the general (i.e., national) government. Created by the general government for macroeconomic purposes, SWFs hold, manage, or administer assets to achieve financial objectives, and employ a set of investment strategies which include investing in foreign financial assets.

5.3.205 Typically, SWFs are established from balance of payments surpluses, proceeds raised from privatisations or revenues from natural resources exports. They are managed to meet specific investment objectives, perhaps for a specific future need. Increasingly in recent years, SWFs have looked to employ third party institutions to assist in the management their assets.

5.3.206 Notwithstanding the different forms that SWFs can take, a large proportion of them are participants in the International Forum of Sovereign Wealth Funds (IFSWF).

5.3.207 The IFSWG was established in April 2009 (succeeding the previous International Working Group) to develop a common set of voluntary principles ("the Santiago Principles") in order to promote a clearer understanding of SWFs through better transparency of their governance and operation. A list of the IFSWF's member funds, and the counties in which they are established, can be found at Appendix II to the Santiago Principles at: http://www.ifswf.org/santiago-principles. Further countries, plus the OECD and the World Bank, participate as permanent observers. The International Monetary Fund provides both a co-chair of the IFSWF and its secretariat.

5.3.208 A general concern exists that SWFs are capable of being used to meet political, rather than purely financial objectives, by acquiring controlling interests in strategically important industries or destabilising economies. For this reason, understanding the nature of purpose of the SWF and the relationship or transaction is a key AML/CTF control and important to the reputation of the firm. Firms should be alert to activities that might give rise to an asset freezing order where UK interests are at stake.

5.3.209 The firm should consider the international reputation of the country and/or SWF concerned (see the Transparency International website

[11] International Forum of Sovereign Wealth Funds *www.ifswf.org*

www.transparency.org for some helpful resources), before entering into a relationship with the fund. Moreover, financial sanctions may be in force against a country that operates an SWF and must be observed irrespective of whether or not the country is a member of the IWG.

5.3.210 SWFs are unlikely to qualify for simplified due diligence.

Nature and legal form

5.3.211 SWFs are constituted in a variety of ways. Usually, however, they take one of the following forms:

- pool of assets managed by the Ministry of Finance or Central Bank;
- government-owned corporation;
- independent corporation established by statute

This means that CDD must be tailored according to the nature of the SWF. A fundamental feature, however, is that the beneficial owner of a SWF is the government concerned.

Obtain standard evidence

5.3.212 The standard evidence outlined below is founded on an SWF's participation in the IFSWF and the close involvement with that body of the OECD, IMF and World Bank. Without the comfort of IFSWF membership, the firm should undertake normal identity verification measures according to the legal form of the SWF.

5.3.213 The following information should be obtained about the identity of the SWF and its officers:

- Full name of the SWF
- Address of the SWF
- Name of the national government
- Names of directors/ trustees (or equivalent)

5.3.214 The objectives in terms of identification are to establish that the SWF exists, that it is owned and controlled by a government and that the individuals with whom the firm has contact in connection with establishing the relationship are bona fide representatives of the fund.

5.3.215 For the purposes of establishing that an SWF exists, reference should normally be made to Appendix II to the Santiago Principles (see paragraph 5.3.207), to confirm that it is represented on the IFSWF as a full or observer member. Additional steps will be required if the fund is not an IFSWF member.

5.3.216 Firms should, where appropriate, verify the identities of the directors (or equivalent) who have authority to give the firm instructions concerning the use or transfer of funds or assets and take steps to be reasonably satisfied that the person(s) the firm is dealing with is properly authorised by the SWF.

5.3.217 To supplement the measures described in paragraph 5.3.216 and assist with the verification of the individuals that represent the fund, a copy of the constitutional documentation should be obtained, including evidence of its establishment or appointment as an SWF and the authority of those individuals to bind the fund or appoint others to do so. Information in the public domain from reputable and independent sources (e.g., news items, international conference programmes etc.) may also be used as additional evidence of an individual's connection with the fund.

5.3.218 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach. Particular care should be exercised if there is a change of government to ensure that the firm is clear as to the individuals authorised to act for the SWF.

Beneficial ownership

5.3.219 SWFs are created to manage the wealth or financial resources at national level so there will be no natural person that has any beneficial interest. The constitutional documents should make this clear.

Nature and purpose

5.3.220 Given the concern that surrounds SWFs (see paragraph 5.3.216), and the fact that those who control them, and perhaps the firm's mandate, are likely in many cases to be PEPs, the firm needs to consider the nature and purpose of various aspects, including:

- the purpose of the SWF
- the purpose of the relationship with the firm
- whether any PEPs are beneficial owners of the SWF, and any heightened ML/TF risk that arises; and
- on an ongoing basis, the reasons for withdrawals from the portfolio

Regulation 33(1)(g) 5.3.221 Each firm's processes should take into account any PEP beneficial ownership of an SWF, and, on a risk-assessed basis, require a person from senior management and independent from the officer sponsoring the relationship to approve the establishment of the relationship. For higher risk relationships, the firm's compliance (or MLRO) function should also satisfy itself that the risks are acceptable.

5.3.222 The purpose of the SWF should be evident from its constitutional documentation and elsewhere. Note that one of Santiago Principles (GAPP 2) is that the purpose of the fund should be clearly defined and publicly disclosed.

5.3.223 The reasons for using the firm's services need to be understood. For example, investment management mandates are likely to be similar to other institutional mandates and should be questioned if they are unusually

focused towards particular sectors, having regard (if appropriate) to the fact that the firm may be managing a specific tranche of the overall fund.

5.3.224 Given the specific nature of SWFs, attention should be given to withdrawals to ensure that the reasons are consistent with the legitimate objectives of the fund and that any payment instructions are appropriate in that context. If the firm has suspicions concerning the motives of the fund, it should make Suspicious Activity Report to the NCA.

5.3.225 Monitoring should be conducted to identify changes to the objectives of the fund and its status in relation to the IFSWF.

Other considerations

5.3.226 When formulating a risk based approach to SWFs, and particularly when considering those based in countries with higher levels of corruption, firms should take into account the fact that some IFSWF member funds may not have fully implemented the Santiago Principles and that observers will not necessarily implement them at all and should factor such variations into their additional enquiries.

5.3.227 If a country is not a member of the IFSWF or does not subscribe to the Santiago Principles, it may be more difficult to obtain information about its constitution and objectives. In these circumstances, the firm must determine what further information, if any, it requires, bearing in mind the need to apply a risk-based approach. For example the firm should understand there may be increased risk that the origins of the fund are corrupt or the funds' purpose constitutes a potential threat in connection with terrorism or economic manipulation.

Pension schemes

5.3.228 UK pension schemes can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations. Many register with HMRC in order to achieve tax-exempt status. Most have to register with the Pensions Regulator. Generally, evidence of registration with HMRC and/or the Pensions Regulator (as relevant on a case-by-case basis) will be sufficient to meet identification and verification obligations in respect of most UK pension schemes. HMRC do not issue approval letters. However, if the firm has any concerns, on application and with the relevant authority, HMRC can be asked to provide documentary confirmation regarding the existence of the scheme. Due to confidentiality restrictions, the Pensions Regulator is unlikely to confirm that a particular pension scheme is registered with them unless the firm is able to provide the scheme's authority for them to provide this information.

Regulation 37(3)(b)(iii)

5.3.229 In determining whether a business relationship presents a low degree of risk of ML/TF, and therefore the extent to which it is appropriate to apply SDD measures, a firm must take into account, inter alia, whether the customer/product is a pension, superannuation or similar scheme which provides retirement benefits for employees, where contributions are made by an employer or by way of deduction from an employee's wages and the

scheme rules do not permit the assignment of a member's interest under the scheme. If the firm determines that the situation presents a low degree of ML/TF risk, simplified due diligence may be applied (see section 5.4).

5.3.230 For such a scheme, therefore, the firm need only satisfy itself that the customer qualifies for simplified due diligence in this way.

Regulation 6(4)(b)(ii)

5.3.231 For a scheme that takes the form of a trust, an individual does not qualify as a beneficial owner through having control solely as a result of discretion delegated to him under s 34 of the Pensions Act 1995.

Obtain standard evidence

5.3.232 Where a pension scheme does not meet the criteria in paragraph 5.3.229, and therefore the firm is not able to determine that simplified due diligence measures may be applied, but has HMRC or Pensions Regulator registration, a firm's identification and verification obligations may be met by confirming the scheme's registration, as described in paragraph 5.3.228.

5.3.233 Where a firm is unable to confirm the scheme's HMRC or Pension Regulator registration, a pension scheme should be treated for AML/CTF purposes according to its legal form and standard evidence obtained. In such circumstances and when a pension scheme is structured as a trust, Regulations 44 and 45(2)(b) of the ML Regulations make it clear that where not all members of the class of beneficiaries have been determined, trustees of such pension schemes need only maintain accurate and up-to-date written records of the class of beneficiaries of the pension scheme (rather than of individual beneficiaries).

Signatories

5.3.234 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Other considerations

5.3.235 Following a risk-based approach, the identity of the principal employer may need to be verified in accordance with the guidance given for companies in paragraphs 5.3.143 to 5.3.176 and the source of funding recorded to ensure that a complete audit trail exists if the employer is wound up.

Payment of benefits

5.3.236 Any payment of benefits by, or on behalf of, the trustees of an occupational pension scheme will not require verification of identity of the recipient. (The transaction will either not be relevant financial business or will be within the scope of the exemption for policies of insurance in respect of occupational pension schemes.)

5.3.237 Where individual members of an occupational pension scheme are to be given personal investment advice, their identities must be verified.

However, where the identity of the trustees and principal employer have been satisfactorily verified (and the information is still current), it may be appropriate for the employer to provide confirmation of identities of individual employees.

Charities, church bodies and places of worship

5.3.238 Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, a Charitable Incorporated Organisation under the Charities Commission, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations.

5.3.239 If the charity is an incorporated entity (or otherwise has legal personality), firms should verify its identity following the guidance in paragraphs 5.3.143ff. The charity itself is the firm's customer, for practical purposes represented by the trustees who give instruction to the firm.

Regulation 6(1)

5.3.240 If the charity takes the form of a trust, it has no legal personality and its trustees have control and management over its affairs. In relation to a trust, the ML Regulations define the settlor (where one exists) and trustees as beneficial owners. Where there is a large number of trustees the firm may take a risk-based approach to determining on how many, and which, in respect of whom the firm should carry out full CDD measures. (see paragraphs 5.3.258ff.)

5.3.241 If the charity takes the form of an unincorporated association, it also has no legal personality. Its officers, or members of its governing body, are then the firm's customers, on whom the firm must carry out full CDD measures. (see paragraphs 5.3.283ff.)

5.3.242 In exceptional cases, another individual may exercise control, such as a receiver appointed to manage the affairs of the charity.

5.3.243 For the vast majority of charities, either there will be no individual who is a beneficial owner (apart from the trustees) within the meaning of the ML Regulations, or at most a class of persons who stand to benefit from the charity's objects must be identified. These persons will be self-evident from a review of the charity's objects in its constitution or the extract from the Register of Charities.

5.3.244 Examples of charities where classes of persons can be identified include charities that relieve poverty, famine or homelessness, educate individuals or alleviate sickness, disability or age. In these cases, a broad description of the class of persons who stand to benefit is sufficient so that the firm understands who the persons are who benefit. Examples of classes might be:

- 'Homeless persons in London'
- 'Deaf and blind people'
- 'Children in the village of Ambridge'

In other charities, no individuals benefit directly from the charity's objects. Examples include charities for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

5.3.245 Neither the Charity Commissioners, nor judges of courts (who may exercise powers over charities) fall within the definition of controllers for these purposes.

Obtain standard evidence

5.3.246 The firm should obtain the following in relation to the charity or church body:

- Full name and address
- Nature of body's activities and objects
- Name(s) of Settlor(s) [if any]
- Names of all trustees (or equivalent)
- Names or classes of beneficiaries

5.3.247 The existence of the charity can be verified from a number of different sources, depending on whether the charity is registered or not, a place of worship or an independent school or college.

Registered charities – England and Wales, and Scotland

5.3.248 The Charity Commission is required to hold a central register of charities in England and Wales and allocates a registered number to each. The Office of the Scottish Charity Regulator carries out a similar function for Scottish charities. When dealing with an application which includes the name of a registered charity, the Charity Commission, or the Office of the Scottish Charity Regulator, can confirm the registered number of the charity and the name and address of the regulator's correspondent for the charity concerned.

5.3.249 Details of all registered charities can be accessed on the Charity Commission website (www.charity-commission.gov.uk), the Office of the Scottish Charity Regulator website (www.oscr.org.uk), or a check can be made by telephone to the respective regulator's enquiry line. Firms should be aware that simply being registered is not in itself a guarantee of the bona fides of an organisation, although it does indicate that it is subject to some ongoing regulation.

Charities in Northern Ireland

5.3.250 Applications from, or on behalf of, charities in Northern Ireland should be dealt with in accordance with procedures for private companies set out in paragraphs 5.3.163 to 5.3.169, if they are limited by guarantee, and for clubs and societies, those in paragraphs 5.3.283 to 5.3.293. Verification of the charitable status can normally be obtained through HMRC.

Church bodies and places of worship

Charities (exception from Registration) Regulations 1996

Registered Places of Worship Act 1855

5.3.251 Certain church bodies are excepted by law from registering as charities and may not therefore have a registered number. For tax purposes, however, they may notify HMRC of their charitable status; verification of their status may be met by having sight of HMRC's confirmation of the church's application for charitable status. The identity of individual churches may be verified through the headquarters or regional organisation of the denomination, or religion.

Unregistered charities or church bodies

5.3.252 Other than those covered by paragraph 5.3.251, the identities of unregistered charities or church bodies, whether in the UK or elsewhere, cannot be verified by reference to registers maintained by independent bodies. Applications from, or on behalf of, unregistered charities should therefore be dealt with in accordance with the procedures for private companies set out in paragraphs 5.3.163 to 5.3.169, for trusts, as set out in paragraphs 5.3.258 to 5.3.282, or for clubs and societies, as set out in paragraphs 5.3.283 to 5.3.293. Firms should take particular note of those paragraphs addressing customers where the money laundering or terrorist financing risk is greater in relation to particular customers, and if it should be followed in these circumstances.

Independent schools and colleges

5.3.253 Where an independent school or college is a registered charity, it should be treated in accordance with the guidance for charities. Any such body which is not registered as a charity should be treated in accordance with the guidance for private companies in paragraphs 5.3.163 to 5.3.169.

5.3.254 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Other considerations

5.3.255 In assessing the risks presented by different charities, a firm might need to make appropriate distinction between those with a limited geographical remit, and those with unlimited geographical scope, such as medical and emergency relief charities.

5.3.256 If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country or jurisdiction, the charity can quite properly be transferring funds to that country or jurisdiction. It would otherwise be less clear why the organisation should be transferring funds to a third country (which may, within the general context of the firm's risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as higher risk.

5.3.257 Non-profit organisations have been known to be abused, to divert funds to terrorist financing and other criminal activities. FATF published a best practices paper on 'Combating the abuse of non-profit organisations' in June 2015 (available at www.fatf-gafi.org), in support of Recommendation 8. In November 2005, the European Commission adopted a Recommendation to member states containing a Framework for a code of conduct for non-profit organisations.

Other trusts and foundations

5.3.258 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 firms 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.

5.3.259 For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the firm, in their capacity as trustees of the particular trust or foundation, are the firm's customers on whom the firm must carry out full CDD measures. Following a risk-based approach, in the case of a large, well known and accountable organisation firms may limit the trustees considered customers to those who give instructions to the firm. Other trustees will be verified as beneficial owners, following the guidance in paragraphs 5.3.8 to 5.3.16.

5.3.260 Most trusts are not separate legal persons, and for AML/CTF purposes should be identified as described in paragraphs 5.3.267 to 5.3.271.

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

5.3.261 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)

5.3.262 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 5.3.261.

Regulation 6(1)(a)(b)

5.3.263 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 42(2)(b)

5.3.264 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.

5.3.265 In some trusts, no individuals may benefit directly; examples include trusts for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

Regulation 6(6),(7)

5.3.266 In relation to a legal entity or legal arrangement which is not a trust the beneficial owners (see paragraph 5.3.262) 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.

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

5.3.267 In respect of trusts, the firm 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 5.3.261, a description of the class of beneficiaries)
- Name of any protector or controller

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

5.3.268 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 5.3.270) to an appropriate register in the country of establishment. The firm must take reasonable measures to understand the ownership and control structure of the customer.

Beneficial owners

Regulation 6(1)(a)(b)

5.3.269 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)

5.3.270 The identities of other beneficial owners (e.g., certain beneficiaries), either individuals or a class, as appropriate, must also be verified (see paragraphs 5.3.8 to 5.3.16). Firms do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a register.

Regulation 6(1)

5.3.271 Where there is a large number of trustees the firm may take a risk-based approach to determining on how many, and which, in respect of whom the firm should carry out full CDD measures. (see paragraphs 5.3.258ff.)

5.3.272 Firms should take appropriate steps to be reasonably satisfied that the person the firm 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.

5.3.273 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

5.3.274 Firms 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.

5.3.275 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 firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Regulation 33(1)(g)

5.3.276 Where a situation is assessed as carrying a higher risk of money laundering or terrorist financing, the firm 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

5.3.277 The guidance in paragraphs 5.3.258 to 5.3.276 applies equally to UK based trusts and non-UK based trusts. On a risk-based approach, a firm will need to consider whether the geographical location of the trust (or

any other risk factor) gives rise to additional concerns, and if so, what they should do.

5.3.278 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."

5.3.279 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.

5.3.280 The nature of a civil law foundation should normally be well understood by firms, or their subsidiaries or branches, operating in the jurisdiction under whose laws the foundation has been set up. Where a foundation seeks banking or other financial services outside its home jurisdiction, firms will need to be satisfied that there are legitimate 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 5.3.267 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.

5.3.281 Where the founder's identity is withheld, firms 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 firm'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.

5.3.282 Whilst firms may conclude on the basis of their due diligence that the request for facilities is acceptable, they should bear in mind that terms like 'foundation', 'stiftung', 'anstalt' are liable to be hijacked by prime bank instrument fraudsters to add spurious credibility to bogus investment schemes.

Clubs and societies

5.3.283 There is a wide variety of clubs and societies, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, to small, local clubs and societies funded by small, individual donations or subscriptions 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 firms take account of the different money laundering or terrorist financing risks that clubs and societies of different sizes, areas of activity and nature of business being conducted, present.

5.3.284 Where an application is made on behalf of a club or society, firms should therefore make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.3.285 Many local clubs and societies are small, with limited resources, and it is important to apply identity verification requirements that are appropriate in the context of the financial crime risk presented by the club or society. This might be particularly relevant in deciding which of the trustees or office holders should be made subject to identity verification.

5.3.286 For the vast majority of clubs and societies, either there will be no individual who is a beneficial owner within the meaning of the ML Regulations, or at most a class of persons who stand to benefit from the club or society's objects must be identified. These persons will be self-evident from a review of the club or society's objects in its constitution.

Obtain standard evidence

5.3.287 For many clubs and societies, the money laundering or terrorist financing risk will be low. The following information should be obtained about the customer:

- Full name of the club/society
- Legal status of the club/society
- Purpose of the club/society
- Names of all officers

5.3.288 The firm should verify the identities of the officers who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets.

5.3.289 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.290 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

5.3.291 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.3.102 to 5.3.106 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.292 The firm's risk assessment may lead it to conclude that the money laundering or terrorist financing risk is higher, and that it should require additional information on the purpose, funding and beneficiaries of the club or society.

5.3.293 Following its assessment of the money laundering or terrorist financing risk presented by the club/society, the firm may decide to verify the identities of additional officers, and/or institute additional transaction monitoring arrangements (see section 5.7).

5.4 Simplified due diligence

Regulation 37(1)

5.4.1 A firm may apply SDD measures in relation to a particular business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low degree of risk of ML/TF.

Regulation 37

5.4.2 When assessing whether there is a low degree of risk of ML/TF in a particular situation, and the extent to which it is appropriate to apply SDD measures in that situation, a firm must take account of at least the following risk factors:

(i) Whether the customer is –
- a public administration, or a publicly owned enterprise 5.3.192/193
- an individual resident in a geographical area of low risk
- a credit or financial institution subject to the requirements in the fourth money laundering directive (see paragraph 5.3.133)
- a company listed on a regulated market (see paragraph 5.3.155)
- firms holding a pooled account (see paragraph 5.3.142)

(ii) certain life assurance and e-money products (see Part II, sectors 7 and 3)

(iii) certain pension funds (see paragraphs 5.4.4 and 5.3.228ff)

(iv) Child Trust Funds and Junior ISAs (see paragraphs 5.4.5 - 5.4.7)

Regulation 37(7)	5.4.3	Annex 5-III to this chapter sets out suggested Risk Factor Guidelines on Simplified Due Diligence, consistent with those issued jointly by the European Supervisory Authorities[12], to which firms must have regard.
Regulation 37(3)(b)(iii)	5.4.4	Subject to an assessment of the ML/TF risk presented, SDD measures may be applied to pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.
Regulation 37(3)(b)(vi)(vii)	5.4.5	SDD measures may be applied to Child Trust Funds and Junior ISAs. .
	5.4.6	In respect of Junior ISAs, although SDD measures may be applied, firms will, however, in due course need to verify identity at the point the child reaches 18 years and becomes entitled to the funds, or at the next 'trigger' event thereafter (unless the child's identity has by then already been verified for the purposes of some other relationship).
	5.4.7	With Junior ISAs, the child is able to manage the account from the age of 16, in which case the firm might choose to undertake customer due diligence at that stage in order to avoid delaying any transaction the child should wish to undertake on reaching 18, when the account becomes a 'full' ISA. It is recommended that firms indicate in their product literature etc. what their policy will be when, for example, the child reaches 16 or 18.
	5.4.8	SDD measures must not be applied, or continue to be applied, where: the firm's risk assessment changes and it no longer considers that there is a low degree of risk of ML/TF; where the firm suspects money laundering or terrorist financing; or where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identity or verification.
Regulation 28(11) POCA s330 (2)(b) Terrorism Act s 21A	5.4.9	A determination that SDD measures may be applied in a particular situation does not remove the obligation to conduct ongoing monitoring of the business relationship, although the extent of this may be adjusted to reflect its determination of the low degree of ML/TF risk. Such determination does not affect the duty to report knowledge or suspicion of money laundering or terrorist financing.
	5.4.10	Firms should also document the rationale for the decision to apply SDD.

[12] These Guidelines were published on 26 June 2017, to take effect by 26 June 2018. See https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

5.5 Enhanced due diligence

Regulation 33 (1)(g)

5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.

5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons:

- to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and
- to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

5.5.3 The extent of additional information sought, and of any monitoring carried out in respect of any particular business relationship, or class/category of business relationship, will depend on the money laundering or terrorist financing risk that the customer, or class/category of business relationship, is assessed to present to the firm.
See 5.5.9 and 5.5.11 for EDD scenarios where additional information must be obtained.

5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

5.5.5 A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The

firm should consider whether, in some circumstances, evidence of source of wealth or income should be required (for example, if from an inheritance, see a copy of the will). The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

5.5.7 The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a firm's understanding of the risk associated with the business relationship. Where appropriate and practical, therefore, and where there are no data protection restrictions, firms should take reasonable steps to ensure that where they have customer due diligence information in one part of the business, they are able to link it to information in another.

5.5.8 At all times, firms should bear in mind their obligations under the Data Protection Act only to seek information that is needed for the declared purpose, not to retain personal information longer than is necessary, and to ensure that information that is held is kept up to date.

Regulation 33(1)

5.5.9 In addition to the general obligation, referred to in paragraph 5.5.1, to apply EDD measures, the ML Regulations prescribe six specific circumstances in respect of which EDD measures must be applied. These are:

- in any case identified by the firm under its risk assessment (or in information provided by the supervisory authorities) where there is a high risk of ML/TF;
- in any business relationship ~~or transaction~~ with a person established in a high risk third country or in relation to any relevant transaction where either of the parties is established in a high risk third country (see 5.5.11);
- in relation to correspondent relationships with a non-EEA credit or financial institution (see Part II, sector 16: *Correspondent relationships*);
- if a firm has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP (see paragraphs 5.5.13ff);
- in any case where a customer has provided false or stolen identification documents or information on establishing a relationship;
- in any case where:
  - a transaction is complex or~~and~~ unusually large; or there is an unusual pattern of transactions, ~~and~~or
  - the transaction or transactions have no apparent economic or legal purpose; or
  - in any case which by its nature presents a higher risk of money laundering or terrorist financing.

Regulation 33(2)

5.5.10 The obligation to apply EDD measures does not apply when the customer is a branch or majority owned subsidiary undertaking located in a high risk country of an entity which is established in an EEA state

and subject to the obligations in the fourth money laundering directive as an obliged entity, if -

- the branch or subsidiary undertaking complies fully with group-wide policies and procedures established by the entity in accordance with the directive; and
- the firm, applying a risk-based approach, does not consider that it is necessary to apply EDD measures.

Regulation 33 (1)(b) and (3)

5.5.11 There are two separate scenarios for which EDD measures must be applied when a high risk third country is involved: Where there is a business relationship with a person established in a high risk third country, and when a firm is undertaking a relevant transaction with a party established in a high risk third country.

A 'high risk third country' means a country which has been identified by the Commission under the fourth money laundering directive as a high risk country. See https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_enThe 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.

Being 'established in' a country for a legal person means being incorporated in or having its principal place of business in that country, for a financial or credit institution it means having its principal regulatory authority in that country, or for an individual it means being resident in that country (not just being born there).

A 'relevant transaction' means a transaction to which a firm must apply CDD measures under Regulation 27. These are occasional transactions that either exceed €15,000 or they are a transfer of fund amounts within the meaning of Article 3.9 of the funds transfer regulation that exceed €1,000.
In this context a relevant transaction therefore relates to an occasional transaction which the firm undertakes for the customer outside of an established business relationship, and does not include ongoing payment activities undertaken within an established business relationship.

In any business relationship with a person established in a high risk third country or in relation to any relevant transaction where either party is established in a high risk third country, EDD measures must include obtaining:

- additional information on the customer and their beneficial owner;
- additional information on the intended nature of the business relationship;
- information of the source of funds and source of wealth of the customer and their beneficial owners;
- information on the reasons for the transactions;

- approval of senior management for establishing and continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls, and selecting patterns of transactions that need further examination.

All of these additional EDD measures must be applied but the extent thereof may be considered and adjusted based on the level of risk of the customer.

Regulation 33(4A) 5.5.12 A firm who is a credit or financial institution must take reasonable measures to identify and verify the identity of the beneficial owners of a life insurance policy before any payment is made under the policy when the customer:

- is a legal person or legal arrangement;
- is the beneficiary of the life insurance policy; and
- presents a high risk of ML/TF for any other reason.

Regulation 33(8) 5.5.132 Annex 5-IV to this chapter sets out suggested Risk Factor Guidelines on Enhanced Due Diligence~~, consistent with those issued jointly by the European Supervisory Authorities[13], to which firms must have regard~~.

Politically exposed persons (PEPs)

Regulation 35(3)(a) 5.5.13 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 firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. 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 5.5.14 The FCA is required to give guidance to the firms it supervises in relation to the EDD measures required under the ML Regulations in respect of PEPs, their family members and known close associates. Firms should have regard to this guidance.

Regulation 35(12)(a) 5.5.15 A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.

Regulation 35(9) 5.5.16 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

~~[13] These Guidelines were published on 26 June 2017, to take effect by 26 June 2018. See https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf~~

longer period as the firm considers appropriate, in order to address risks of ML/TF in relation to that person.

Regulation 35(14)

5.5.17 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 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.

5.5.18 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, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Regulation 35(12)(b)

5.5.19 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)

5.5.20 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)

5.5.21 A firm is no longer obliged to apply EDD measures 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 5.5.16 has expired.

Regulation 35(15)

5.5.22 For the purpose of deciding whether a person is known to be a close associate of a PEP, the firm need only have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose an active research by the firm.

Regulation 35(1), (5)

5.5.23 Firms are required, on a risk-sensitive basis, 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 establishing, or continuing, a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

Risk-based procedures

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

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

5.5.25 Firms should take a proportional, risk-based and differentiated approach to conducting transactions or business relationships with PEPs, depending on where they are assessed on the scale of risk.

5.5.26 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)

5.5.27 In order to determine how to assess individual customers for PEP purposes, firms' analysis should therefore employ an appropriate risk-based approach, to assess where on the PEP continuum an individual lies. Firms 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 firms to take less intrusive and less exhaustive EDD measures.

5.5.28 Where firms 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. Resources such as the Transparency International Corruption Perception Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in terms of assessing the risk. The IMF, World Bank and some non-governmental organisations also publish relevant reports. If there is a need to conduct more thorough checks, or if there is a high likelihood of a firm having PEPs for customers, subscription to a specialist PEP database may be an adequate risk mitigation tool.

Source of wealth

5.5.29 It is for each firm to decide the steps it takes to determine whether a PEP is seeking to establish a business relationship for legitimate reasons.

Regulation 35(5)(b)

5.5.30 Firms must take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures firms 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, and where the individual sits on the PEP continuum. Firms 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.

5.5.31 Firms 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[14]. Firms should note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Firms 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.

5.5.32 For PEPs who are assessed as being higher on the scale of risk, firms 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, firms could seek evidence of conveyancing.

Senior management approval

5.5.33 Obtaining approval from senior management for establishing, or continuing, a business relationship 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

[14] 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

dictates, firms should escalate decisions to more senior management levels.

5.5.34 The appropriate level of seniority for sign off should therefore be determined by the level of increased risk associated with the business relationship; and the senior manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the firm'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 firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively.

On-going monitoring

5.5.35 Guidance on the on-going monitoring of the business relationship is given in section 5.7. Firms should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The firm should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, EDD measures must be applied to that customer.

5.5.36 Firms should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring and review should be determined by the level of risk associated with the relationship.

5.6 Multipartite relationships, including reliance on third parties

5.6.1 Frequently, a customer may have contact with two or more firms in respect of the same transaction. This can be the case in both the retail market, where customers are routinely introduced by one firm to another, or deal with one firm through another, and in some wholesale markets, such as syndicated lending, where several firms may participate in a single loan to a customer.

5.6.2 However, several firms requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience of the customer. It is important, therefore, that in all circumstances each firm is clear as to its relationship with the customer and its related AML/CTF obligations, and as to the extent to which it can rely upon or otherwise take account of the verification of the customer that another firm 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 firms involved may not be UK-based.

5.6.3 In other cases, a customer may be an existing customer of another regulated firm in the same group. Guidance on meeting AML/CTF obligations in such a relationship is given in paragraphs 5.6.24 to 5.6.27.

Reliance on third parties

Regulation 39

5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 39(3) (see paragraph 5.6.6). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.5 For example:

- where a firm (firm A) enters into a business relationship with, or undertakes an occasional transaction for, the underlying customer of another firm (firm B), for example by accepting instructions from the customer (given through Firm B); or
- firm A and firm B both act for the same customer in respect of a transaction (e.g., firm A as executing broker and firm B as clearing broker),

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

Regulation 39(3)

5.6.6 In this context, Firm B must be:

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

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

(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;

(4) an organisation whose members consist of persons within (1), (2) and (3) above.

Regulation 39(2)(a)

5.6.7 Where a firm relies on a third party to carry out CDD measures, it must immediately obtain from the third party all the information needed to identify the customer or beneficial owner.

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

5.6.8 The firm must enter into arrangements with the firm being relied on which:

- Enable the firm 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 8.12 and 8.18).

Regulation 39(7)(8)

5.6.9 Nothing in the ML Regulations prevents a firm applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 5.6.13 to 5.6.16), provided that the arrangements between the firm and the agent or outsourcing service provider provide for the firm to remain liable for any failure to apply such measures.

Basis of reliance

5.6.10 For one firm to rely on verification carried out by another firm, the verification that the firm 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 SDD carried out, or any other exceptional form of verification, such as the use of source of funds as evidence of identity.

5.6.11 Firms may also only rely on verification actually carried out by the firm being relied upon. A firm that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another firm.

Regulation 10(2)(a),

5.6.12 Under the ML Regulations, the FCA has the additional responsibility for supervising the AML/CTF systems and controls in Annex I Financial Institutions. Such businesses are not regulated by the FCA, and may not therefore be relied on to carry out CDD measures on behalf of other firms until such time as this is permitted under the ML Regulations.

5.6.13 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming 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, the product/service sought and the sums involved;
- any adverse experience of the other firm's general efficiency in business dealings;
- any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

5.6.14 The assessment as to whether or not a firm 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.

5.6.15 In practice, the firm 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.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance is given in paragraphs 5.6.29 to 5.6.30 below on the use of pro-forma confirmations containing the above information.

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

5.6.17 For a firm to confirm that it has carried out CDD measures in respect of a customer is a serious matter. A firm must not give a confirmation on the basis of a generalised assumption that the firm'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.

Regulation 40(7)

5.6.18 A firm (other than an agent or outsourced service provider) which is relied on by another person must, if requested by the firm relying on it, immediately

- make available to the firm which is relying on it any information about the customer (and any beneficial owner) which the third party obtained when applying CDD measures; and
- forward to the firm which is relying on it copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures

5.6.19 The personal information supplied by the customer as part of a third party's customer identification procedures will generally be set out in the form that the relying firm will require to be completed, and this information will therefore be provided to that firm.

Regulation 40 (6), (7)

5.6.20 A request to forward copies of any identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained when applying CDD measures, if made, would normally be as part of a firm's risk-based customer acceptance procedures. However, the firm giving the confirmation must be prepared to provide these data or other relevant documents throughout the period for which it has an obligation under the Regulations to retain them.

5.6.21 Where a firm makes such a request, and it is not met, the firm will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future.

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

5.6.23 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 39(3) (see paragraph 5.6.6).

Group introductions

Regulation 39(6)

5.6.24 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group which first dealt with the customer. One member of a group should be able to confirm to another part of the group that the identity of the customer has been appropriately verified.

Regulation 39(5)

5.6.25 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for his identity to be re-verified, provided that:

- the identity of the customer has been verified by the introducing part of the group in line with AML/CTF standards in the UK, the EU or an assessed low risk jurisdiction; and
- the group entity that carried out the CDD measures can be relied upon as a third party under Regulation 39(3).

5.6.26 The acceptance by a UK firm of confirmation from another group entity that the identity of a customer has been satisfactorily verified is dependent on the relevant records being readily accessible, on request, from the UK.

5.6.27 Where UK firms have day-to-day access to all group customer information and records, there is no need to obtain a group introduction confirmation, if the identity of that customer has been verified previously to AML/CTF standards in the EU, or in an assessed low risk jurisdiction. However, if the identity of the customer has not previously been verified, for example because the group customer relationship pre-dates the introduction of anti-money laundering regulations, or if the verification evidence is inadequate, any missing verification evidence will need to be obtained.

Use of pro-forma confirmations

Regulation 39 (3)

5.6.28 Whilst a firm may be able to place reliance on another party to apply all or part of the CDD measures under Regulation 39(3) (see paragraph 5.6.4), 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 a firm is unlikely to have an ongoing 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 5.6.18).

5.6.29 Pro-forma confirmations for customer identification and verification are attached as Annex 5-I to this chapter.

5.6.30 Pro-forma confirmations in respect of group introductions are attached as Annex 5-II to this chapter.

Situations which are not reliance

(i) One firm acting solely as introducer

5.6.31 At one end of the spectrum, one firm may act solely as an introducer between the customer and the firm providing the product or service, and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the firm, and has no relationship with either of these parties that would constitute a business relationship. This would be the case, for example, in respect of name-passing brokers in inter-professional markets, on which specific guidance is given in Part II, sector 19: *Name passing brokers in the inter-professional market.*

5.6.32 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the ML Regulations lie with the product/service provider. This does not, of course, preclude the introducing firm carrying out identification and verification of the customer on behalf of the firm providing the product or service, as agent for that firm (see paragraphs 5.6.34 – 5.6.35).

(ii) Where the intermediary is the agent of the product/service provider

5.6.33 If the intermediary is an agent or appointed representative of the product or service provider, it is an extension of that firm. The intermediary may actually obtain the appropriate verification evidence in respect of the customer, but the product/service provider is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

5.6.34 Similarly, where the product/service provider has a direct sales force, they are part of the firm, whether or not they operate under a separate group legal entity. The firm is responsible for specifying what is required, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

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

5.6.35 From the point of view of a product/service provider, the position of 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. Guidance on assessing which countries or jurisdictions might be low risk jurisdictions is given at Annex 4-I.

Regulation 37(1)

5.6.36 Depending on jurisdiction, where the customer is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, and the firm determines that the situation presents a low degree of risk of ML/TF, the product provider may decide to carry out SDD measures on both the customer and on the underlying party (see paragraph 5.3.134).

5.6.37 Where a firm cannot apply simplified due diligence to the intermediary (see paragraphs 5.4.1ff), the product/service provider is obliged to carry out CDD measures on the intermediary and, as the intermediary acts for another, on the underlying customer.

5.6.38 Where the firm takes instruction from the underlying customer, or where the firm acts on the underlying customer's behalf (e.g., as a custodian) the firm then has an obligation to carry out CDD measures in respect of that customer, although the reliance provisions (see paragraphs 5.6.4ff) may be applied.

5.6.39 In these circumstances, in verifying the identity of the underlying customer, the firm should take a risk-based approach. It will need to assess the AML/CTF regime in the intermediary's jurisdiction, the level of reliance that can be placed on the intermediary and the verification work it has carried out, and as a consequence, the amount of evidence that should be obtained direct from the customer.

5.6.40 In particular, where the intermediary is located in a higher risk jurisdiction, or in a country listed as having material deficiencies, the risk-based approach should be aimed at ensuring that the business does not proceed unless the identity of the underlying customers have been verified to the product/service provider's satisfaction.

5.7 Monitoring customer activity

The requirement to monitor customers' activities

Regulation 28(11)

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. 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 firm'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.

5.7.2 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 firms know

their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

What is monitoring?

5.7.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

5.7.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken

and in either case, unusual transactions or activities will be flagged for further examination.

5.7.5 Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

5.7.6 Firms should also have systems and procedures to deal with customers who have not had contact with the firm for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorised use.

5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

Nature of monitoring

5.7.9 Some financial services business typically involves transactions with customers about whom the firm has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the firm may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of

the firm, the frequency of customer activity, and the types of customers that are involved.

5.7.10 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country; and
- the parties concerned: for example, a request to make a payment to or from a person on a sanctions list.

5.7.11 The arrangements should include the training of staff on procedures to spot and deal specially (e.g., by referral to management) with situations that arise that suggest a heightened money laundering risk; or they could involve arrangements for exception reporting by reference to objective triggers (e.g., transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity.

Regulation 33(1), 33(5)(d)

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

Manual or automated?

5.7.13 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced. One or other of these approaches may suit most firms. In the relatively few firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary.

5.7.14 It is essential to recognise the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer, cannot be automated (see Chapter 8: Staff awareness, training and alertness).

5.7.15 In relation to a firm's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the outputs of the system are appropriate. Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.

5.7.16 The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some automation. Systems available include those that many firms, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud

monitoring systems can often indicate possible money laundering or terrorist financing.

5.7.17 There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems available are not designed to detect money laundering or terrorist financing, but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.

5.7.18 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for firms to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that should be addressed include:

- How does the solution enable the firm to implement a risk-based approach to customers, third parties and transactions?
- How do system parameters aid the risk-based approach and consequently affect the quality and volume of transactions alerted?
- What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the firm's particular line of business?
- What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
- What functionality exists to provide the user with the reason that a transaction is alerted and is there full evidential process behind the reason given?
- Does the system have robust mechanisms to learn from previous experience and how is the false positive rate continually monitored and reduced?

5.7.19 What constitutes unusual or uncharacteristic behaviour by a customer, is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the firm.

5.7.20 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is

important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of 'false positives', which require excessive resources to investigate.

5.7.21 Monitoring also involves keeping information held about customers up to date, as far as reasonably possible. Guidance on this is given at paragraphs 5.3.27 - 5.3.28.

ANNEX 5-I/1

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY A UK-REGULATED FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer:
[tick only one]

meets the standard evidence set out within the Guidance for the UK Financial Sector issued by JMLSG ; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FCA Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-I/2

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY AN EU REGULATED FINANCIAL SERVICES FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, on request from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Money Laundering Directive

ANNEX 5-I/3

CONFIRMATION OF VERIFICATION OF IDENTITY
PRIVATE INDIVIDUAL

INTRODUCTION BY A NON-EU REGULATED FINANCIAL SERVICES FIRM (which the receiving firm has accepted as being from an assessed low risk jurisdiction)

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

We confirm that:

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, on request from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1 A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.

2 This form cannot be used to verify the identity of any customer that falls into one of the following categories:

- those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of local anti money laundering laws or regulation requiring such verification; or
- those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering laws or regulation.

ANNEX 5-I/4

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY A UK-REGULATED FIRM

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer: [tick only one]

meets the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FCA Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-I/5

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY AN EU REGULATED FINANCIAL SERVICES FIRM

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. “Relevant company registry” includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
    - those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Money Laundering Directive

ANNEX 5-I/6

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY A NON-EU REGULATED FINANCIAL SERVICES FIRM

(which the receiving firm has accepted as being from an assessed low risk jurisdiction)

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that:

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1 "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.

2 This form cannot be used to verify the identity of any customer that falls into one of the following categories:

- those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of local anti money laundering laws or regulation requiring such verification; or
- those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering laws or regulation.

ANNEX 5-II/1

CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION
PRIVATE INDIVIDUAL

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer		
Current Address		Previous address if customer has changed address in the last three months
Date of Birth		

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

i. of the Money Laundering Regulations 2017, and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

ii. of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

iii. of local law and regulation.

(b) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-II/2

CONFIRMATION OF VERIFICATION OF IDENTITY

GROUP INTRODUCTION

CORPORATE AND OTHER NON-PERSONAL ENTITY

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

(i) of the Money Laundering Regulations 2017, and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

(ii) of our national money laundering legislation that implements the EU Money Laundering Directive, and any authoritative relevant guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

(iii) of local law and regulation.

(b) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-III

RISK FACTOR GUIDELINES

Simplified Due Diligence

Firms may apply simplified due diligence (SDD) measures in situations where the ML/TF risk associated with a business relationship is low. SDD is not an exemption from any of the CDD measures; however, firms may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they identified.

SDD measures firms may apply include, but are not limited to:

- adjusting the timing of CDD, for example where the product or transaction sought has features that limit its use for ML/TF purposes, such as:

  (i) verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or

  (ii) verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Firms must make sure that:

    a) this does not result in a *de facto* exemption from CDD, i.e. firms must ensure that the customer or beneficial owner's identity will ultimately be verified;

    b) the threshold or time limit is set at a reasonably low level;

    c) they have systems in place to detect when the threshold or time limit has been reached; and

    d) they do not defer CDD or delay obtaining relevant information about the customer where applicable legislation does not permit this.

- adjusting the quantity of information obtained for identification, verification or monitoring purposes, such as:

  (i) verifying identity on the basis of one document only; or

  (ii) assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping centre gift card.

- adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example:

  (i) accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; note that this is not permitted in relation to the verification of the customer's identity;

  (ii) where the risk associated with all aspects of the relationship is determined to be very low, relying on the source of funds to meet some of the CDD requirements, *e.g.* where the funds are state benefit payments or where the

funds have been transferred from an account in the customer's name at an EEA firm.

- adjusting the frequency of CDD updates and reviews of the business relationship, for example only when trigger events occur such as the customer looking to take out a new product or service, or when a certain transaction threshold is reached; firms must make sure that this does not result in a *de facto* exemption from keeping CDD information up-to-date.

- adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions which, taken together, would exceed that threshold.

The information a firm obtains when applying SDD measures must enable the firm to be reasonably satisfied that the risk associated with the relationship is low. It must also be sufficient to give the firm enough information about the nature of the business relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering or terrorist financing is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied.

ANNEX 5-IV

RISK FACTOR GUIDELINES

Enhanced due diligence

Unusual transactions

Firms should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a firm detects transactions that are unusual because:

- they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs; or
- they have an unusual or unexpected pattern compared to the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- they are very complex compared to other, similar transactions by similar customer types, products or services,

and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply EDD measures.

These EDD measures should be sufficient to help the firm determine whether these transactions give rise to suspicion and must at least include:

- taking reasonable measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate with the risk it has identified.

High risk jurisdictions and other high risk situations

When dealing with individuals or entities established or residing in a high risk third country identified by the Commission, EDD measures must be applied (see 5.5.1). ~~and in~~ In all other high risk situations, firms should take an informed decision which EDD measures are appropriate for each high risk situation and the~~. The~~ appropriate type of EDD (~~,~~ including the extent of additional information sought, and ~~of the~~ increased monit)~~ monitoring carried out~~, will depend on the reason why a relationship was classified as high risk.

Firms will not need to apply all EDD measures listed below in all cases. For example, in certain high risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

EDD measures firms should apply may include:

- increasing the quantity of information obtained for CDD purposes:

(i) about the customer's or beneficial owner's identity, or the customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:

a. information about family members and close business partners;

b. information about the customer's or beneficial owner's past and present business activities; and

c. adverse media searches.

(ii) about the intended nature of the business relationship, to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. It includes obtaining information on:

a. the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions. In some cases, requesting evidence may be appropriate;

b. why the customer looks for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;

c. the destination of funds; or

d. the nature of the customer's or beneficial owner's business to understand the likely nature of the business relationship better.

- increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity including by:

(i) requiring the first payment to be carried out through an account verifiably in the customer´s name with a bank subject to UK CDD standards; or

(ii) establishing that the customer's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with the firm's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly increased, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The sources of funds or wealth can be verified, among others, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports.

- increasing the frequency of reviews, to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship or conclude that it no longer corresponds to its risk appetite and to help identify any transactions that require further review, including by:

(i) increasing the frequency of reviews of the business relationship, to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;

(ii) obtaining the approval of senior management to commence or continue the business relationship to ensure senior management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

(iii) reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon; or

(iv) conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions.