

The Joint Money Laundering Steering Group



Prevention of
money
laundering/
combating
terrorist financing

2017 REVISED VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR
PART II: SECTORAL GUIDANCE

June 2017 [Amended December 2017]

© JMLSG. All rights reserved.

For permission to copy please contact JMLSG.

Any reproduction, republication, transmission or reuse in whole or part requires our consent.

Draftsman/Editor: David Swanney

CONTENTS**PART II: SECTORAL GUIDANCE**

This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Sector

1	Retail banking
1A	Money service businesses (as customers of banks)
2	Credit cards, etc
3	Electronic money
4	Credit unions
5	Wealth management
6	Financial advisers
7	Life assurance, and life-related pensions and investment products
7A	General insurers
8	Non-life providers of investment fund products
9	Discretionary and advisory investment management
10	Execution-only stockbrokers
11	Motor finance
11A	Consumer credit providers
12	Asset finance
13	Private equity
14	Corporate finance
15	Trade finance
16	Correspondent banking
17	Syndicated lending
18	Wholesale markets
19	Name-passing brokers in inter-professional markets
20	Brokerage services to funds
21	Invoice finance

1: Retail banking

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 1.1 Retail banking is the provision of standard current account, loan and savings products to personal and business customers by banks and building societies. It covers the range of services from the provision of a basic bank account facility to complex money transmission business for a medium sized commercial business. In this guidance, retail banking does not cover credit cards, which are dealt with in sector 2. For many firms, retail banking is a mass consumer business and will generally not involve close relationship management by a named relationship manager.
- 1.2 This sectoral guidance refers primarily to business undertaken within the UK. Firms operating in markets outside the UK will need to take account of local market practice, while at the same time ensuring that equivalent CDD and record-keeping measures to those set out in the ML Regulations are applied by their branches and subsidiary undertakings operating in these markets.

What are the money laundering and terrorist financing risks in retail banking?

- 1.3 There is a high risk that the proceeds of crime will pass through retail banking accounts at all stages of the money laundering process. However, many millions of retail banking transactions are conducted each week and the likelihood of a particular transaction involving the proceeds of crime is very low. A firm's risk-based approach will therefore be designed to ensure that it places an emphasis within its strategy on deterring, detecting and disclosing in the areas of greatest perceived vulnerability.
- 1.4 There is an increasing risk of fraudulent applications by identity thieves. However, such applications represent a very small percentage of overall applications for retail banking services.
- 1.5 The provision of services to cash-generating businesses is a particular area of risk associated with retail banking. Some businesses are legitimately cash based, including large parts of the retail sector, and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify, thus providing grounds for looking more closely at whether the account may be being used for money laundering or terrorist financing.
- 1.6 The feature of lending is generally that the initial monies advanced are paid into another bank or building society account. Consolidation loans may involve payment direct to the borrower's creditor, and the amount borrowed in some unsecured lending arrangements may be taken in cash. Repayments are usually made from other bank or building society accounts by direct debit; in most cases, repayments in cash are not encouraged.
- 1.7 Given that a loan results in the borrower receiving funds from the lender, the initial transaction is not very susceptible of the placement stage of money laundering, although it could form part

FINAL BOARD APPROVED

of the layering stage. The main money laundering risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination.

- 1.8 Where loans are made in one jurisdiction, and collateral is held in another, this may indicate an increased money laundering risk.

Other relevant industry and regulatory guidance

- 1.9 Firms should make use of other existing guidance and leaflets etc. in this area, as follows:
- See “Fighting Financial Crime” pages on www.fca.org.uk
 - “International Students – opening a UK bank account” and “Guidance for people wanting to manage a bank account for someone else – see www.bba.org.uk
- 1.10 See also paragraphs 1.39 – 1.42 on financial exclusion.

Customer due diligence

General

- 1.11 The AML/CTF checks carried out at account opening are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals opening accounts or obtaining services from banks. Firms should co-ordinate these processes, in order to provide as strong a gatekeeper control as possible.
- 1.12 For the majority of personal applicants, sole or joint, the standard identification evidence set out in Part I, Chapter 5 will be applicable, including, in the case of customers not met face to face, consideration of the additional precautions set out in paragraphs 5.3.85 – 5.3.90. See also 1.36 below.
- 1.13 Documents that are acceptable in different situations are summarised in Part I, paragraphs 5.3.70 – 5.3.75, together with the principles defining when reliance may be placed on a single document or where more than one is required. A current UK passport or photocard driving licence (containing an in-date photograph – see Part I, paragraph 5.3.77) issued in the UK is likely to be used in the majority of cases, other than in the context of financial exclusion, where a bespoke token may be accepted, as set out in Annex 1-I. Non-UK nationals entering the UK should present their national passports or national identity cards, other than in the context of financial exclusion, where bespoke tokens are referred to in Annex 1-I for refugees and asylum seekers.
- 1.14 Electronic verification may be also used to meet a firm’s customer identification obligations. However, a firm should first consider whether electronic verification is suitable for its customer base, and should then have regard to the guidance in Part I, paragraphs 5.3.40-5.3.45 and 5.3.79-5.3.84. When using electronically-sourced evidence to verify identity, firms should ensure that they have an adequate understanding of the data sources relied on by the external agencies that supply the evidence. Firms should be satisfied that these sources provide enough cumulative evidence to provide reasonable certainty of a person’s identity, and conform with the guidance set out in Part I, Chapter 5. An electronic check that accesses a single database (e.g., Electoral Register check) is normally not enough on its own to verify identity.
- 1.15 The other documents cited in Part I, paragraph 5.3.76 may be used for UK residents where the standard documents are not available, whether singly or in conjunction, according to the principles set out in that paragraph. For non-UK residents, or persons who have recently entered

FINAL BOARD APPROVED

the UK, firms may well require additional documentary evidence - not for AML/CTF purposes, but to offset fraud and credit risks which would normally be addressed through electronic checks for UK residents (see paragraphs 1.23-1.25).

- 1.16 Where a firm determines that a particular business relationship or transaction presents a low degree of risk of ML/TF, having taken into account the risk assessment the firm has carried out and the risk factors referred to in Regulation 36(3) (see Part I, paragraph 5.4.2), simplified customer due diligence measures may be applied. Simplified due diligence may also be considered in the following situations:
- Where the source of funds may be used as evidence of identity. See Part I, paragraphs 5.3.102 to 5.3.106.
 - Where a variation from the standard is required to prevent a person from being financially excluded (see paragraphs 1.39 – 1.42 and Annex 1-I).
 - Products which meet the criteria in Regulation 37(3)(b) of the ML Regulations 2017, e.g., a Junior ISA
- 1.17 However, a firm should take care with customers whose identity is verified under a variation from the standard and who wish to migrate to other products in due course. The verification of identity undertaken for a basic bank account may not be sufficient for a customer migrating to a higher risk product. Firms should have processes defining what additional due diligence, including where appropriate further evidence of identification, is required in such circumstances.
- 1.18 Where the incentive to provide a false identity is greater, firms should consider deploying suitable fraud prevention tools and techniques to assist in alerting to false and forged identification. Where the case demands, a firm might require proof of identity additional to the standard evidence.

A customer with an existing account at the same firm

- 1.19 If the existing customer was taken on pre-1994, or it could not be established that the customer's identity had previously been verified, an application would trigger standard identification procedures.
- 1.20 If the customer's identity has been verified to a standard commensurate with the risk associated with the business relationship, a second account would normally be opened without further identification procedures, (provided the characteristics of the new account are not in a higher risk category than the existing account). Thus, a foreign currency account might require further identification procedures and/or additional customer enquiries but for a new savings account, where the applicant's existing account had been subject to adequate CDD checks, most firms would not require further identification.

Customers with a bank account with one firm who wish to transfer it to another

- 1.21 Standard identification procedures will usually apply. In some cases, the firm holding the existing account may be willing to confirm the identity of the account holder to the new firm, and to provide evidence of the identification checks carried out. Care will need to be exercised by the receiving firm to be satisfied that the previous verification procedures provide an appropriate level of assurance for the new account, which may have different risk characteristics from the one held with the other firm.

FINAL BOARD APPROVED

- 1.22 Where different UK regulated firms in the same group share a customer and (before or after any current customer review) transfer a customer between them, either firm can rely on the other firm's review checks in respect of that customer. Care will need to be exercised by the receiving part of the group to be satisfied that the previous verification procedures provide an appropriate level of assurance for the new account, which may have different risk characteristics from the one held with the other part of the group.

Non-resident, physically present in the UK, wishing to open a bank account

- 1.23 A non-resident, whether a non-UK national or a UK national who is returning to the UK after a considerable absence, who is physically present in the UK and who wishes to open an account should normally be able to provide standard identification documentation to open a Basic Bank Account (see Part I, paragraph 5.3.76 and Annex 1-I).

Non-resident, not physically present in the UK, wishing to open a bank account

- 1.24 Non-residents not physically resident in the UK wishing to open an account in the UK are entitled to open a Basic Bank Account, with its limited facilities. Such a customer may fall within the firm's criteria for wealth management clients, in which case the guidance in sector 5: *Wealth Management* will apply. Enhanced due diligence may apply where other high risk factors, such as where the customer is not met personally, come into play (see paragraphs 5.17-22 and Part I, section 5.5).

Members of HM Diplomatic Service returning to the UK and wishing to open a bank account.

- 1.25 The standard identification evidence, as set out in Part I Chapter 5, should be able to be obtained in these cases. Members of HM Diplomatic Service are, however, reported to have experienced difficulties in opening a bank account because, for example, they have no recent electronic data history stored in the UK. Account opening procedures may be facilitated by a letter from the Foreign Office confirming that the person named was a member of the Diplomatic Service and was returning to the UK.

Lending

- 1.26 Many applications for advances are made through brokers, who may carry out some of the customer due diligence on behalf of the lender. In view of the generally low money laundering risk associated with mortgage business and related protection policies, and the fraud prevention controls in place within the mortgage market, use of confirmations from intermediaries introducing customers is, in principle, perfectly reasonable, where the introducer is carrying on appropriately regulated business (see Part I, paragraph 5.6.6) including appointed representatives of FCA authorised firms.
- 1.27 Firms should refer to the guidance on situations where customers are subject to identification by two or more financial services firms in relation to the same transaction, set out in Part I, section 5.6.

Business Banking

- 1.28 Business banking in the Retail sector is by nature a volume business, typically offering services for smaller UK businesses, ranging from sole traders and small family concerns to partnerships, professional firms and smaller private companies (e.g.. turnover under £1million pa). These businesses are often, but not always, UK-based in terms of ownership, location of premises and customers. As such, the risk profile may actually be lower than that of larger businesses with a more diverse customer base or product offering, which may include international business and

FINAL BOARD APPROVED

customers. The profile may, however, often be higher than that of personal customers, where identification may be straightforward and the funds involved smaller.

- 1.29 Essentially, as set out in Part I, Chapter 5, identification should initially focus on ascertaining information about the business and its activities and verifying beneficial owners holding or controlling directly or indirectly, 25% or more of the shares or voting rights, and controllers, and where the business is a limited company, obtaining and verifying the information on the basis set out in Regulation 28(3) in respect of the company.
- 1.30 Uncertainties may often arise with a business that is starting up and has not yet acquired any premises (e.g., X & Y trading as ABC Ltd, working from the director/principal's home). A search of Companies House may not always produce relevant information if the company is newly formed.
- 1.31 In the case of newly-formed businesses, obtaining appropriate customer information is sometimes not easy. The lack of information relating to the business can be mitigated in part by making sufficient additional enquiries to understand fully the customer's expectations (nature of proposed activities, anticipated cash flow through the accounts, frequency and nature of transactional activity, an understanding of the underlying ownership of the business) and personal identification of the owners/controllers of the business, as well as information on their previous history. Part I, Chapter 5, contains further guidance relating to identification standards.
- 1.32 Firms may encounter difficulties with validating the business entity, particularly where directorships may not have been registered or updated. It is recommended that where this arises (and firms still feel able to open an account on the basis of the evidence already seen) firms conduct or take additional steps to confirm the control and ownership of the business after the account has been opened, by checking to ensure directorships have been updated. Where mitigating steps have been taken to compensate for information not being easily available, firms should consider the probability that additional monitoring of the customer's transactions and activity should be put in place.
- 1.33 A firm must be reasonably satisfied that the persons starting up the business are who they said they are, and are associated with the firm. Reasonable steps must be taken to verify the identity of the persons setting up a new business, as well as any beneficial owners, which may often be based on electronic checks. In the majority of cases, the individuals starting up a business are likely to be its beneficial owners. A check of the amount of capital invested in the business, whether it is in line with the firm's knowledge of the individual(s) and whether it seems in line with their age/experience, etc, may be a pointer to whether further enquiries need to be made about other possible beneficial owners.
- 1.34 Wherever possible, documentation of the firm's business address should be obtained. Where the firm can plausibly argue that this is not possible because it is in the early stages of start-up, the address of the firm should be verified later; in the interim, the bank may wish to obtain evidence of the address(es) of the person(s) starting up the business. In certain circumstances, a visit to the place of business may be helpful to confirm the existence and activities of the business.
- 1.35 In determining the identification appropriate for partnerships (see Part I, paragraphs 5.3.177 - 5.3.191), whose structure and business may vary considerably, and will include professional firms e.g. solicitors, accountants, as well as less regulated businesses, it will be important to ascertain where control of the business lies, and to take account of the risk inherent in the nature of the business.

FINAL BOARD APPROVED

Enhanced due diligence

1.36 Enhanced due diligence is required under Regulation 33 of the ML Regulations in the following situations:

- When the business, or other aspect, of the customer relationship is determined to present a high risk of money laundering or terrorist financing. Examples should be set out in the firm's risk-based approach and should reflect the firm's own experience and information produced by the authorities. See Part I, paragraphs 4.59 – 4.69 and section 5.5 for general guidance.
- When the proposed customer relationship or transaction is with a person established in a high risk non-EEA country;
- When establishing a correspondent relationship with an institution in a non-EEA state (although in practice most firms would not regard such relationships as forming part of their 'retail' business).
- When the applicant is a PEP, or a family member or close associate of a PEP. See Part I, paragraphs 5.5.13 - 5.5.31.
- Where a customer has provided false or stolen identification documentation or information on establishing a relationship;
- Where:
 - A transaction is complex and unusually large, or
 - There is an unusual pattern of transactions, and
 The transaction has no apparent economic or legal purpose.

1.37 Firms will need to consider making more penetrating initial enquiries, over and above that usually carried out before taking on businesses whose turnover is likely to exceed certain thresholds, or where the nature of the business is higher risk, or involves large cash transactions. *Recognising that there are a very large number of small businesses which are cash businesses, there will be constraints on the practicality of such enquiries; even so, firms should be alert to the increased vulnerability of such customers to laundering activity when evaluating whether particular transactions are suspicious.* Examples of higher risk situations are:

- High cash turnover businesses: casinos, bars, clubs, taxi firms, launderettes, takeaway restaurants
- Money service businesses: cheque encashment agencies, bureaux de change, money transmitters
- Gaming and gambling businesses
- Computer/high technology/telecom/mobile phone sales and distribution, noting especially the high propensity of this sector to VAT 'Carousel' fraud
- Companies registered in one offshore jurisdiction as a non-resident company with no local operations but managed out of another, or where a company is registered in a high risk jurisdiction, or where beneficial owners with significant interests in the company are resident in a high risk jurisdiction
- Unregistered charities based or headquartered outside the UK, 'foundations', cultural associations and the like, particularly if centred on certain target groups, including specific ethnic communities, whether based in or outside the UK (see FATF Typologies Report 2003/4 under 'Non-profit organisations' – at www.fatf-gafi.org)

1.38 Firms should maintain and update customer information, and address any need for additional information, on a risk-sensitive basis, under a trigger event strategy (for example, where an existing customer applies for a further product or service) or by periodic file reviews.

Financial exclusion

FINAL BOARD APPROVED

- 1.39 Denying those who are financially excluded from access to the financial sector is an issue for deposit takers. Reference should be made to the guidance given in Part I, paragraphs 5.3.121 to 5.3.125, and Annex 1-I.
- 1.40 The “financially excluded” are not a homogeneous category of uniform risk. 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 any additional customer information, or monitoring 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.
- 1.41 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 Part I, 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.
- 1.42 Where an applicant produces non-standard documentation, staff should be discouraged from citing the ML Regulations as an excuse for not opening an account before 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. Staff should bear in mind that the ML Regulations are not explicit as to what is and is not acceptable evidence of identity.

Monitoring

- 1.43 Firms should note the guidance contained in Part I, section 5.7, and the examples of higher risk businesses in paragraph 1.37. It is likely that in significant retail banking operations, some form of automated monitoring of customer transactions and activity will be required. However, staff vigilance is also essential, in order to identify counter transactions in particular that may represent money laundering, and in order to ensure prompt reporting of initial suspicions, and application for consent where this is required.
- 1.44 Particular activities that should trigger further enquiry include lump sum repayments outside the agreed repayment pattern, and early repayment of a loan, particularly where this attracts an early redemption penalty.
- 1.45 Mortgage products linked to current accounts do not have a predictable account turnover, and effective rescheduling of the borrowing – which can be repaid and re-borrowed at the borrower’s initiative – does not require the agreement of the lender. This should lead to the activity on such accounts being more closely monitored.
- 1.46 In a volume business, compliance with the identification requirements set out in the firm’s policies and procedures should also be closely monitored. The percentage failure rate in such compliance should be low, probably not exceeding low single figures. Repeated failures in excess of this level by a firm over a period of time may point to a systemic weakness in its identification procedures which, if not corrected, would be a potential breach of FCA Rules and should be reported to senior management. This should be part of the standard management information that a firm collates and provides to MLRO and other senior management.

FINAL BOARD APPROVED***Training***

- 1.47 Firms should note the guidance contained in Part I, Chapter 7. In the retail banking environment it is essential that training should ensure that branch counter staff are aware that they must report if they are suspicious. It should also provide them with examples of red flags to look out for.

Reporting

- 1.48 Firms should note the guidance contained in Part I, Chapter 6. As indicated in Part I, paragraphs 7.32 to 7.40, further reference material and typologies are available from the external sources cited, viz: FATF and NCA websites. In addition, firms should be aware of the requirement under Section 331(4) of the Proceeds of Crime Act for reports to be submitted “as soon as practicable” to NCA.
- 1.49 There is no formal definition of what “as soon as practicable” means, but firms should note the enforcement action taken by the FCA in respect of the anti money laundering procedures in place at a large UK firm. The FCA imposed a financial penalty on the firm due, in part, to finding that over half of the firm’s suspicious activity reports were submitted to NCA more than 30 days after having been reported internally to the firm’s nominated officer. In view of the volumes of reports which may be generated in this sector, firms may wish to keep under review whether their nominated officer function is adequately resourced. It is reasonable to base the timescale not on the date that an alert is generated but rather the point in time at which, following internal investigation, a determination is made that it is suspicious and should be reported to NCA. In all circumstances, however, firms should ensure that their end to end process is as efficient as it can be.

Interbank Agency Agreements

- 1.50 Staff in one firm (firm A) may become suspicious of a transaction undertaken over their counters by a customer of another firm (firm B), as might arise under an Interbank Agency Agreement, which permits participating banks to service other banks' customers. In such a case, a report should be made to the nominated officer of firm A, who may alert the nominated officer of firm B. In each case, the nominated officer will need to form their own judgement whether to disclose the circumstances to NCA.

ANNEX 1-I

Special Cases

Many customers in the categories below will be able to provide standard documents, and this will normally be a firm's preferred option. This annex is a non-exhaustive and non-mandatory list of documents (see Notes) which are capable of evidencing identity for special cases who either cannot meet the standard verification requirement, or have experienced difficulties in the past when seeking to open accounts, and which will generally be appropriate for opening a Basic Bank Account. These include:

Customer	Document(s)
Benefit claimants	Entitlement letter issued by DWP, HMRC or local authority, or Identity Confirmation Letter issued by DWP or local authority
Those in care homes/sheltered accommodation/refuge	Letter from care home manager/warden of sheltered accommodation or refuge Homeless persons who cannot provide standard identification documentation are likely to be in a particular socially excluded category. A letter from the warden of a homeless shelter, or from an employer if the customer is in work, will normally be sufficient evidence.
Those on probation	It may be possible to apply standard identification procedures. Otherwise, a letter from the customer's probation officer, or a hostel manager, would normally be sufficient.
International students	Passport or EEA National Identity Card AND Letter of Acceptance or Letter of Introduction from Institution on the UK Border Agency list (see http://www.bia.homeoffice.gov.uk/employers/points/). See the pro forma agreed for this purpose with UKCOSA: The Council for International Education, attached as Annex 1-II. See also Part I, paragraphs 5.3.118-119.
Prisoners	It may be possible to apply standard identification procedures. Otherwise, a letter from the governor of the prison, or, if the applicant has been released, from a police or probation officer or hostel manager would normally be sufficient. See the pro forma agreed for this purpose with the National Offender Management Service and UNLOCK, attached as Annex 1-III
Economic migrants [<i>here meaning those working temporarily in the UK, whose lack of banking or credit history precludes their being offered other than a basic bank account</i>]	National Passport, or National Identity Card (nationals of EEA and Switzerland) Details of documents required by migrant workers are available at www.employingmigrants.org.uk and Home Office website https://www.gov.uk/government/organisations/home-office Firms are not required to establish whether an applicant is legally entitled to work in the UK but if, in the course of checking identity, it came to light that the applicant was not

FINAL BOARD APPROVED

	entitled to do so, the deposit of earnings from employment could constitute an arrangement under the Proceeds of Crime Act.
Refugees (those who are not on benefit)	<p>Immigration Status Document with Biometric Residence Permit, or IND travel document (i.e., <i>Blue</i> Convention Travel doc, or <i>Red</i> Stateless Persons doc, or <i>Brown</i> Certificate of Identity doc)</p> <p>Refugees are unlikely to have their national passports and will have been issued by the Home Office with documents confirming their status. A refugee is normally entitled to work, to receive benefits and to remain in the UK.</p>
Asylum seekers	<p>IND Application Registration Card (ARC) <i>NB This document shows the status of the individual, and does not confirm their identity</i></p> <p>Asylum seekers are issued by the Home Office with documents confirming their status. Unlike refugees, however, information provided by an asylum seeker will not have been checked by the Home Office. The asylum seeker's Applicant Registration Card (ARC) will state whether the asylum seeker is entitled to take employment in the UK. Asylum seekers may apply to open an account if they are entitled to work, but also to deposit money brought from abroad, and in some cases to receive allowances paid by the Home Office.</p> <p>Firms are not required to establish whether an applicant is legally entitled to work in the UK but if, in the course of checking identity, it came to light that the applicant was not entitled to do so, the deposit of earnings from employment could constitute an arrangement under the Proceeds of Crime Act.</p>
Travellers	Travellers may be able to produce standard identification evidence; if not, they may be in a particular special case category. If verification of address is necessary, a check with the local authority, which has to register travellers' sites, may sometimes be helpful.

Notes:

1. Passports, national identity cards and travel documents must be current, i.e. unexpired. Letters should be of recent date, or, in the case of students, the course dates stated in the Letter of Acceptance should reasonably correspond with the date of the account application to the bank. All documents must be originals. In case of need, consideration should be given to verifying the authenticity of the document with its issuer.
2. As with all retail customers, firms should take reasonable care to check that documents offered are genuine (not obviously forged), and where these incorporate photographs, that these correspond to the presenter.
3. Whilst it is open to firms to impose additional verification requirements if they deem necessary under their risk based approach and to address the perceived commercial risks attaching to their

FINAL BOARD APPROVED

own Basic Account products, they should not lose sight of the requirement under *SYSC 6.3.7 (5) (G)* “not unreasonably [to] deny access to its service to potential customers who cannot reasonably be expected to provide detailed evidence of identity.”

(To be typed on education institution letterhead)

LETTER OF INTRODUCTION FOR UK BANKING FACILITIES

We confirm that..... *(Please insert Student's FULL Name)* is/will be studying at the above named education institution.

Course Details

Name of Course:

Type of Course:

Start Date:

Finish Date:

Address Details [if known]

The Student's Overseas Residential Address is:
(Please insert the Student's full Overseas Address)

.....
.....
.....

We have/have not (please delete whichever is applicable) corresponded with the Student at their above overseas address.

The Student's UK Address is: [if known]

(Please insert the Student's UK Address)

.....
.....
.....
.....

This certificate is only valid if embossed with the education institution's seal or stamp.

Signed.....

Name.....

Position.....

Contact Telephone Number at education institution.....



Ministry of
JUSTICE

National Offender
Management Service

PERSONAL IDENTIFICATION DOCUMENT

I am willing for this form to be passed to [*insert name of bank*] to help me to apply for a Basic bank account, and to notify the bank of the address I will be living at when I am released.

Name.....

Nationality Place of Birth.....

Signature..... Date.....

Upon my release I will be living at the following address. I understand that I *must* confirm my address to the bank within 7 days of my release from custody. (*If the address is not known at time of completing the application this section must be completed when known, and confirmed at the Discharge Board (any changes must be communicated to the bank).*)

.....

.....

Witnessed by

.....

Position of witness [*must* be an employee of the prison]

.....

Signature of witness

.....

FINAL BOARD APPROVED

The following sections must be signed by an authorised manager

Applicant's Full Name

.....

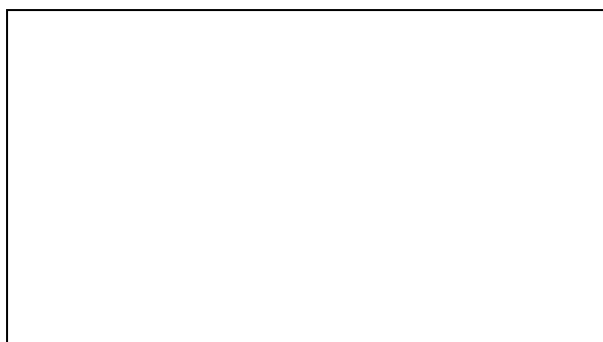
Applicant's Date of Birth

Applicant's Current Address (HMP/YOI)

.....

.....

Applicant's Photograph (to be affixed here)



Expected Release Date.....

Address immediately prior to custody

.....

.....

Verification of name and address by HMP

I certify that the name and address details supplied above match those on the court/prison records related to the applicant shown above.

I confirm that the photograph is a true likeness of the applicant.

NamePosition

e-mail address@hmpr.gov.uk

Direct telephone line

Signature Date

1A: Money service businesses (as customers of banks)*Overview of the sector*

	1A.1	The MSB industry is extremely diverse, ranging from large international companies with numerous outlets worldwide to small, independent convenience stores in communities with population concentrations that do not necessarily have access to traditional banking services or in areas where English is rarely spoken.
	1A.2	The range of products and services offered, and the customer bases served by MSBs, are equally diverse. Indeed, while they all fall under the definition of a money services business, the types of businesses are quite distinct. Some MSBs offer a variety of services, whilst others only offer money services as an ancillary component to their primary business, such as a convenience store that cashes cheques or a hotel that provides currency exchange.
	1A.3	MSB services can include one or more of the following activities: <ul style="list-style-type: none"> ➤ Currency dealing/exchanging; ➤ Cheque cashing; ➤ Money remitting; and ➤ Issuing, selling and redeeming stored value and monetary instruments, such as money orders and traveller's cheques.
Regs 54, 56, 58	1A.4	Under the ML Regulations, MSBs are required to register with HMRC in order to be able to carry out their activities, unless they are subject to FCA supervision. Registration is subject to the MSB meeting the 'fit and proper' test set out in the ML Regulations, which from 26 June 2017 is also applied to an MSB's agents.
Reg 3(3)(a) Sch 1 Sch 2(1)(e)	1A.5	Where MSBs carry out money transmission services, they are included within the definition of financial institutions, and are therefore subject to the full provisions of the ML Regulations. The exemption from the ML Regulations for activities that are engaged in only on an occasional or very limited basis does not apply to money transmission services.
SI 209/2009 Reg 6	1A.6	Under the Payment Services Regulations 2009, MSBs carrying out money remittance services must be included on a register maintained by the FCA. MSBs on the register can be: <ul style="list-style-type: none"> • Authorised Payment Institutions (which are required to meet certain minimum standards in respect of capital, management and systems and controls, and whose client funds must be kept in a separate client account with an authorised bank); or • Small Payment Institutions (which are exempt from minimum capital requirements, but whose management must meet certain requirements on propriety and experience, and whose

business level must be less than a prescribed monthly maximum); or

- Agents of an API or an SPI.

1A.7 Many different business models can be used to make money remittance payments, each carrying different AML/CTF risks. Several of these are described on the UKMTA website at www.ukmta.org.

Reg 23(1)(d)(ii)
Reg 25(1)(b), 25(3),
26(1)(b)

1A.8 MSBs may be subject to supervision by the FCA for AML/CTF, if they are part of a banking or financial services group. Other MSBs are supervised by HMRC, which must maintain a register of those MSBs it supervises, and this register may in future be made available for public inspection. MSBs must not operate unless they are supervised by the FCA or registered with HMRC. Confirmation that a particular MSB is on the HMRC register may be found at <https://customs.hmrc.gov.uk/msbregister/checkTerms.do> (but this website does not allow access to the whole register itself).

What are the money laundering and terrorist financing risks in MSBs?

1A.9 Several features of the MSB sector make it an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as the simplicity and certainty of MSB transactions, worldwide reach (in case of money remitters), the cash character of transactions, low thresholds, the often less stringent customer identification rules that are applied to low value transactions compared with opening bank accounts and reduced possibilities for verification of the customer's identification than in credit or other financial institutions. The nature of the underlying customer's relationship with the MSB and a low frequency of contact with them can also be a significant vulnerability.

1A.10 Generally, MSBs can be used for money laundering and terrorist financing in two ways: either by wittingly or unwittingly performing relevant transactions for their customers without knowledge of the illegal origin or destination of the funds concerned, or by a direct involvement of the staff/management of the provider through complicity or through the ownership of such businesses by a criminal organisation.

1A.11 MSBs can be used at all stages of the money laundering process. Currency exchanges specifically are an important link in the money laundering chain. Once the money has been exchanged, it is difficult to trace its origin. Also, considering that many are small businesses, currency exchanges can be more easily prone to takeover by criminals and used to launder money.

1A.12 Obtaining ownership of an MSB either directly or via sub-agent relationships provides criminals a perfect tool to manipulate the money transfer system and to launder money. Detecting such cases depends, to a certain extent, on the firm applying CDD measures and monitoring/reporting obligations effectively.

1A.13 The following indicators could be relevant in this context:

- Reluctance by the MSB to provide information about the identity of their customers when requested by the bank;
- Use of false identification and fictitious names for customers;
- Turnover of the MSB exceeding, to a large extent, the cash flows of other comparable businesses in the sector;
- Suspicious connections of the MSB owner;
- Suspicious transactions performed on the bank accounts of the MSB or its owner;
- Suspicion that a business (such as a travel agent or corner shop) is actually providing MSB services to the customers of its primary business, or leveraging another business name/type to cover up unregistered activity;
- Overly complicated agent/principal networks (e.g. multiple principals for one agent, agents with their own agents etc.) with inadequate oversight by principal.

1A.14 A survey carried out by FATF suggests the most important factors that may indicate possible misuse of MSBs include:

- Use of underground remittance systems;
- Mismatch between the economic activity, country of origin, or person and the money remittances received;
- Periodic transfers made by several people to the same beneficiary or related persons;
- Transfers over a short period of time of low amounts that together represent a large sum of money;
- Transfers from one or more senders in different countries to a local beneficiary;
- Sudden inflow of funds in cash followed by sudden outflow through financial instruments such as drafts and cheques;
- Structuring of transactions and/or changing of MSB for subsequent orders to keep a low profile; and
- False information during the customer identification procedure/lack of co-operation.

1A.15 Many reported cases of abuse involve small value wire transfers (although some involve high-value amounts), but the total value of funds involved in these cases can be quite significant, raising the possible involvement of organised criminal activity.

Risk assessment

1A16 The risk inherent in the MSB sector is not the nature of the sector itself, but the potential for the abuse of the sector by criminals. It is therefore important that firms understand these potential risks, and manage them effectively. This risk will be greater in some MSBs than in others, and firms should be able to carry out a risk assessment that allows such a judgement to be made.

1A.17 As a part of a risk-based approach, 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 their risk assessment processes, and thus manage their 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.

1A.18 A firm should establish whether the MSB is itself regulated for money laundering/terrorist financing prevention and, if so, whether the MSB is required to verify the identity of its customers and apply other AML/CTF controls – in the case of a non-UK MSB, whether these obligations and controls are to UK standards, or to standards equivalent to those laid down in the money laundering directive. How UK based customers deal with non-UK MSBs can be relevant – especially if there is a non face to face element in the relationship.

1A.19 A firm should determine whether the MSB business is a principal in its own right, or whether it is itself an agent of another MSB. MSBs which operate as principal, or through a limited number of offices/agents present a different risk profile from MSBs which operate through a network of agents – it is important to understand the way the latter type of MSB monitors and confirms compliance by its agents with the AML/CTF controls it lays down.

1A.20 MSBs which carry out periodic internal or external audits or reviews of their AML/CTF controls, including those at its branches and agents, demonstrate a more pro-active management of their ML/TF profile. The outcome of such audits or reviews will be of interest to firms.

1A.21 The information about an MSB that firms should consider obtaining as part of their risk assessment includes

➤ Types of products and services offered

In order to assess risks, firms should know the categories of money services engaged in by the particular MSB customer.

➤ Maturity of the business, and its owners' experience

It is relevant to consider whether or not the MSB is a new or established operation, the level of experience the management and those running the business have in this type of activity, and whether or not providing money services are the customer's primary, or an ancillary, business.

➤ Location(s) and market(s) served

Money laundering risks within an MSB can vary widely depending on the locations, customer bases, and markets served. Relevant considerations include whether markets served are domestic or

international, or whether services are targeted to local residents or to broad markets. For example, a convenience store that only cashes payroll or government cheques generally presents a lower money laundering risk than a cheque casher that cashes any type of third-party cheque or cashes cheques for commercial enterprises (which generally involve larger amounts).

➤ Anticipated account activity

Firms should ascertain the expected services that the MSB will use, such as currency deposits or withdrawals, cheque deposits, or funds transfers. For example, an MSB may only operate out of one location and use only one branch of the firm, or may have several agents making deposits at multiple branches throughout the firm's network. Firms should also have a sense of expected transaction amounts.

➤ Purpose of the account

Firms should understand the purpose of the account for the MSB. For example, a money transmitter might require the bank account to remit funds to its principal clearing account or may use the account to remit funds cross-border to foreign-based agents or beneficiaries. Accounts for use in the MSBs remittance business should be separate from accounts used for the administration of the MSB itself.

1A.22 As with any category of customer, there will be some MSBs that present lower risks of money laundering compared with those that pose a significant risk. Firms should therefore take a risk based approach and neither define nor treat all MSBs as intrinsically posing the same level of risk. Put simply, a convenience store that also cashes payroll cheques for customers purchasing groceries cannot be equated with a money transmitter specialising in cross-border wire transfers to jurisdictions posing heightened risk for money laundering or the financing of terrorism, and therefore the AML obligations on firms will differ significantly.

1A.23 Annex 1A-I lists factors that might indicate a lower, or higher, risk of ML/TF in MSBs.

Customer due diligence

About the customer

Regulation 5(c)

1A.24 The firm should ensure that it fully understands the MSB's legal form, structure and ownership, and must obtain sufficient additional information on the nature of the MSB's business, and the reasons for seeking the product or service.

1A.25 It is important to know and understand any associations the MSB 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.

Ownership and control

- | | | |
|------------------------------------|-------|---|
| Regulation 5(b) | 1A.26 | 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. |
| Regulation 6(1)
Regulation 5(b) | 1A.27 | 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 MSB's shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. The firm must take risk based and adequate measures to verify the identity of those individuals (see Part I, paragraphs 5.3.11 and 5.3.12). Verifying the identity of the beneficial owner(s) 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. |
| | 1A.28 | Following the firm's assessment of the money laundering or terrorist financing risk presented by the MSB, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals (Part I, paragraphs 5.3.57 to 5.3.105). 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 Part I, paragraph 5.3.126). |
| | 1A.29 | Part I, paragraphs 5.3.129 – 5.3.132 refer to the standard evidence for corporate customers, and Part I, paragraphs 5.3.133 – 5.3.139 provide further supplementary guidance on steps that may be applied as part of a risk-based approach. |

Nature and purpose of the relationship

- | | | |
|-----------------|-------|---|
| Regulation 5(c) | 1A.30 | A firm must understand the purpose and intended nature of the business relationship 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 on-going monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard. |
| | 1A.31 | Depending on the firm's risk assessment of the situation, information that might be relevant may include some or all of the following: <ul style="list-style-type: none"> ➤ record of changes of address; |

FINAL BOARD APPROVED

- the expected source and origin of the funds to be used in the relationship;
- the origin of the initial and on-going source(s) of wealth and funds of the MSB;
- 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, on each account to be opened;
- the MSB's settlement arrangements, including the relationship with parties in the second and third miles.

1A.32 In the light of the risk it perceives in the proposed customer, a firm 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.

MSB's AML/CTF policies

1A.33 HMRC has issued guidance to MSBs on their AML/CTF obligations. As with any other customer subject to AML obligations, the extent to which a firm should enquire about the existence and operation of the anti-money laundering programme of a particular MSB will be dictated by the firm's assessment of the risks of the particular relationship. Given the diversity of the MSB industry and the risks they face, there may be significant differences among AML programmes of MSBs. The resources and experience available within the MSB's compliance function and, in a principal/agent situation, how the principal ensures and monitors compliance with the AML/CFT standards in their agents, are also relevant.

1A.34 In the light of the information that the firm has on the MSB's AML/CTF policies and procedures, it should consider what further steps it should take to be comfortable that these policies are reasonable and effective, possibly including seeing the results of an audit or review of the MSB's AML/CTF policies and procedures.

Enhanced due diligence (EDD)

Regulation 14(1)(b)

1A.35 A firm's due diligence should be commensurate with the level of risk of the MSB customer identified through its risk assessment. If a firm's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be required to conduct further due diligence in a manner commensurate with the heightened risk.

FINAL BOARD APPROVED

- 1A.36 Whenever faced with less transparency 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.
- 1A.37 While the extent to which firms should perform further due diligence beyond the minimum will be dictated by the level of risk posed by the particular customer, it is not the case that all MSBs will always require additional due diligence. In some cases, no further customer due diligence will be required - in other situations, however, the further due diligence required may be extensive. In all cases, the level of due diligence applied will be dictated by the risks associated with the particular customer.
- 1A.38 Depending on the level of perceived risk, and the size and sophistication of the particular MSB, firms may pursue a range of actions as part of an appropriate due diligence review or risk management assessment of an MSB seeking to establish an account relationship. Similarly, if the firm becomes aware of changes in the profile of the MSB to which services are being provided, additional steps may be appropriate. Firms will not uniformly require any or all of the actions identified for all MSB customers.
- 1A.39 Where the customer is an overseas, unregulated MSB (see 1A.42 if a UK MSB), additional due diligence should be undertaken to ascertain and assess the effectiveness of the MSB's internal policy on money laundering/terrorist financing prevention and its CDD and activity monitoring controls and procedures. In larger cases, where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to UK or equivalent standards. If not, the extent to which the parent's controls meet UK or equivalent standards, and whether these are communicated and enforced 'effectively' throughout its network of international offices, should be ascertained.
- 1A.40 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 provided, request additional information, for example as to the MSB's activities, customer base or ownership, in order to decide whether to continue with the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of higher-risk business relationships.

On-going monitoring

Reg 8

- 1A.41 Firms are required to conduct on-going monitoring of business relationships, and to identify and report known or suspected suspicious activity or transactions. Risk-based monitoring of accounts maintained for all customers, including MSBs, is a key element of an effective system to identify and, where appropriate, report suspicious activity. The level and frequency of such monitoring will depend, among other

things, on the firm's risk assessment and the activity across the account. The firm may require that a regular (or periodic) audit or review of the MSB's AML/CTF controls is carried out.

- 1A.42 Based on the firm's assessment of the risks of its particular MSB customer, monitoring should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time. The mere existence of unusual transactions does not necessarily mean that a problem exists, but may be an indication that additional review is necessary. Furthermore, risk-based monitoring generally does not include "real-time" monitoring of all transactions flowing through the account of an MSB, such as a review of the payee or drawer of every deposited cheque.
- 1A.43 Examples of unusual activity across MSB accounts, that may or may not be potentially suspicious generally involving significant unexplained variations in transaction size, nature, or frequency through the account, could include:
- A cheque casher depositing cheques from financial institutions in jurisdictions posing heightened risk for money laundering or the financing of terrorism or from countries identified as having weak anti-money laundering controls when the MSB does not overtly market to individuals related to the particular jurisdiction;
 - A cheque casher seeking to deposit currency. Given that a cheque casher would typically deposit cheques and withdraw currency to meet its business needs, any deposits of currency may be an indicator of suspicious activity;
 - A money transmitter transferring funds to a different jurisdiction from expected based on the due diligence information that the firm had assessed for the particular money services business. For example, if the money transmitter represented to the firm or in its business plan that it specializes in remittances to Latin America and starts transmitting funds on a regular basis to another part of the world, the unexplained change in business practices may be indicative of suspicious activity; or
 - A money transmitter or seller/issuer of money ordering deposits currency significantly in excess of expected amounts, based on the due diligence information that the firm had assessed for the particular MSB, without any justifiable explanation, such as an expansion of business activity, new locations, etc.
- 1A.44 Given the importance of the requirement for MSBs to register, a firm should file a suspicious activity report if it becomes aware that an MSB is operating without registration with HMRC, or authorisation by the FCA.
- 1A.45 There is no requirement in the ML Regulations that a firm must close an account that is the subject of a suspicious activity report. Firms are therefore not expected automatically to terminate existing accounts of MSBs based solely on the discovery that the customer is an MSB that

has failed to comply with registration requirements (although continuing non-compliance by the MSB may be an indicator of heightened risk). In these circumstances, further enquiries ought to be made.

ANNEX 1A-I

RISK INDICATORS

To assist firms in determining the level of risk posed by an MSB as a customer, the following are examples that may be indicative of lower and higher risk, respectively. In determining the level of risk, a firm should not take any single indicator as determinative of the existence of lower or higher risk. Moreover, the application of these factors is fact-specific, and a conclusion regarding an account should be based on a consideration of available information.

An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

Examples of potentially lower risk indicator:

The MSB –

- primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;
- offers only a single line of money services business product (for example, only cheque cashing or only currency exchanges);
- is a cheque casher that does not accept cheques drawn on foreign banks;
- is a cheque casher that only cashes payroll or government cheques;
- is an established business with a known operating history;
- only provides services such as cheque cashing to local residents;
- is a money transmitter that only remits funds to domestic entities; or
- only facilitates domestic bill payments.

Examples of potentially higher risk indicator:

The MSB –

- allows customers to conduct higher-amount transactions with moderate to high frequency;
- offers multiple types of money services products;
- is a cheque casher that cashes cheques for commercial businesses;
- is a money transmitter that offers only, or specialises in, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls or to countries subject to detailed and large scale financial sanction regimes;
- is a currency dealer or exchanger for currencies of jurisdictions posing heightened risk for money laundering or the financing of terrorism or countries identified as having weak anti-money laundering controls;
- is a new business without an established operating history;
- is a relatively small concern, with few staff but is a principal with a large agent network - this mitigates against effective supervision and control of agents ;
- the MSB has agents who have agents of their own, or the principal is itself an agent of another business; or
- carries out third party trade based settlements as part of the clearance process.

2: Credit cards, etc

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 2.1 A credit card evidences an unsecured borrowing arrangement between an issuing entity and a cardholder, whereby the cardholder obtains goods and services through merchants approved by the Merchant Acquirer (see paragraph 2.9), up to an agreed credit limit on the card. Cards may also be used at ATMs to withdraw cash, which is then added to the balance owing on the card account. Withdrawals (charged to the card account) across a bank counter may be made, upon the presentation of sufficient evidence of identity.
- 2.2 The cardholder agrees to repay any borrowing, in full or in part, at the end of each statement period. There will be a minimum monthly repayment figure (typically between 2% and 3% of the outstanding balance, depending on the issuer). Interest is charged by the issuing entity, at an agreed rate, on any borrowing not repaid at the end of each period. Any interest or fees charged are added to the card balance.
- 2.3 Cards are issued by individual Card Issuers, each of whom is a member of one or more Card Schemes (e.g., Visa, MasterCard). Each credit card will be branded with the logo of one of the card schemes, and may be used at any merchant worldwide that displays that particular scheme logo. Cash may also be withdrawn through ATMs which bear the scheme logo.
- 2.4 Credit cards may be used through a number of channels. They may be used at merchants' premises at the point of sale, or may be used remotely over the telephone, web or mail (referred to as 'card not present' use). In card not present use, additional security numbers shown on the card may or may not be required to be used, depending on the agreement between merchant and its acquiring bank. The Merchant Acquirer (see paragraph 2.9) will undertake its own assessment of the merchant, and decide what type of delivery channel(s) it will allow the merchant to use to accept card transactions.

Different types of credit card

- 2.5 A Card Issuer may have a direct relationship with the cardholder, in which case the card will clearly indicate the names of the Issuer and of the cardholder. Some Issuers also issue and manage cards branded in the name of other firms (referred to as 'branded cards'), and/or which carry the name of another organisation (referred to as 'affinity cards'). Each card scheme has strict rules about the names that must appear on the face of each card.
- 2.6 Store cards are similar to credit cards, but are issued in the name of a retail organisation, which is not a member of a card scheme. These cards may be issued and operated by a regulated entity within the store group, or on their behalf by other firms that issue and operate other cards. Store cards may only be used in branches of the store, or in associated organisations, and not in other outlets. Generally, store cards cannot be used to obtain cash. They are therefore limited to the domestic market, and cannot be used internationally.
- 2.7 As well as issuing cards to individuals, an Issuer may provide cards to corporate organisations, where a number of separate cards are provided for use by nominated employees of that organisation. The corporate entity generally carries the liability for the borrowings accrued under their employees' use of their cards, although in some cases the company places the

FINAL BOARD APPROVED

primary liability for repayment on the employee (generally to encourage the employee to account for his expenses, and to claim reimbursement from the company, in a timely manner).

- 2.8 This sectoral guidance applies to all cards that entitle the holder to obtain unsecured borrowing, whether held by individuals or corporate entities, and whether these are straightforward credit cards, branded or affinity cards, or store cards. It is not intended to apply to pre-paid cards (although in terms of processing these would use the same infrastructure as credit and debit cards), which are dealt with in sector 3: *Electronic money*.

Merchant acquisition

- 2.9 Merchant Acquirers provide a payment card processing service, which facilitates acceptance of payment card transactions between cardholders and merchants. Payment cards that bear card scheme acceptance brands (e.g., MasterCard and Visa) are issued by banks and financial institutions which are members of the relevant card scheme. The Merchant Acquirer processes the card transaction on behalf of its merchant customer, including, in appropriate cases, seeking authorisation for the transaction from the card issuer.
- 2.10 Payment (settlement) is made by the Card Issuer through the Card Scheme – e.g., Visa. In turn the scheme will pass funds to the Merchant Acquirer through the merchant's bank account. The merchant is therefore a customer of (i) the acquiring bank for the purposes of transaction processing, and (ii) the bank with which it maintains its primary banking relationship, which may or may not be the same as the acquirer. The merchant does not have a relationship with the Card Issuer. For further guidance on transactions through Merchant Acquirers, see Part III, sector 1: *Transparency in electronic payments*, paragraph 1.18.
- 2.11 At the outset of the relationship with the merchant, the Merchant Acquirer will gather information on such matters as the expected card turnover, and average ticket value. This information is assessed in respect to the type of business the merchant is undertaking and the size of such business.

What are the money laundering and terrorist financing risks in issuance of credit cards?

- 2.12 Credit cards are a way of obtaining unsecured borrowing. As such, the initial risks are more related to fraud than to 'classic' money laundering; but handling the criminal property arising as a result of fraud is also money laundering. Card Issuers will therefore generally carry out some degree of credit check before accepting applications.
- 2.13 The money laundering risk relates largely to the source and means by which repayment of the borrowing on the card is made. Payments may also be made by third parties. Such third party payments, especially if they are in cash or by debit cards from different locations or accounts, represent a higher level of money laundering risk than when they come from the cardholder's bank account by means of cheque or direct debit.
- 2.14 Balances on cards may move into credit, if cardholders repay too much, or where merchants pass credits/refunds across an account. Customers may ask for a refund of their credit balance. Issuance of a cheque by a Card Issuer can facilitate money laundering, as a credit balance made up of illicit funds could thereby be passed off as legitimate funds coming from a regulated firm.
- 2.15 Where a cardholder uses his card for gambling purposes (although the use of credit cards is prohibited in casinos), a card balance can easily be in credit, as scheme rules require that winnings are credited to the card used for the bet. It can be difficult in such circumstances to identify an unusual pattern of activity, as a fluctuating balance would be a legitimate profile for such a cardholder.

FINAL BOARD APPROVED

- 2.16 Cash may be withdrawn in another jurisdiction; thus a card can enable cash to be moved cross-border in non-physical form. This is in any event the case in respect of an amount up to the credit limit on the card. Where there is a credit balance, the amount that may be moved is correspondingly greater; it is possible for a cardholder to overpay substantially, and then to take the card abroad to be used. However, most card issuers limit the amount of cash that may be withdrawn, either in absolute terms, or to a percentage of the card's credit limit.
- 2.17 Where several holders are able to use a card account, especially to draw cash, the Card Issuer may open itself to a money laundering or terrorist financing risk in providing a payment token to an individual in respect of whom it holds no information. The issuer would not know to whom it is advancing money (even though the legal liability to repay is clear), unless it has taken some steps in relation to the identity of all those entitled to use the card. Such steps might include ascertaining:
- whether the primary or any secondary cardholder (including corporate cardholders) is resident in a high-risk jurisdiction or, for example, a country identified in relevant corruption or risk indices (such as Transparency International's Corruption Perception Index) as having a high level of corruption
 - whether any primary or secondary cardholder is a politically exposed person and, if so, the nature and extent of any money laundering/terrorist financing risk associated with them. Fuller guidance on the treatment of PEPs is provided in Part I, section 5.5.

Managing the elements of risk

- 2.18 Measures that a firm might consider for mitigating the risk associated with a credit card customer base include the following:
- deciding whether to disallow persons so identified in the above two categories, or to subject them to enhanced due diligence, including full verification of identity of any secondary cardholder
 - requiring the application process to include a statement of the relationship of a secondary cardholder to the primary cardholder based on defined alternatives (eg. Family member, carer, none)
 - deciding whether either to disallow as a secondary cardholder on a personal account any relationship deemed unacceptable according to internal policy parameters, or where the address of the secondary cardholder differs to that of the primary cardholder, or to subject the application to additional enquiry, including verification of the secondary cardholder
 - becoming a member of closed user groups sharing information to identify fraudulent applications, and checking both primary and secondary cardholder names and/or addresses against such databases
 - deciding whether to decline to accept, or to undertake additional or enhanced due diligence on, corporate cardholders associated with an entity which is engaged in a high-risk activity, or is resident in a high-risk jurisdiction, or has been the subject of (responsible) negative publicity
 - implementing ongoing transaction monitoring of accounts, periodic review and refinement of the parameters used for the purpose. Effective transaction monitoring is the key fraud and money laundering risk control in the credit card environment
 - in the event that monitoring or suspicious reporting identifies that a secondary cardholder has provided significant funds for credit to the account, either regularly or on a one-off basis, giving consideration to verifying the identity of that secondary cardholder where it has not already been undertaken
 - deciding whether the cardholder should be able to withdraw cash from his card account

FINAL BOARD APPROVED

- deciding whether the card may be used abroad (and monitoring whether it is used abroad)

Who is the customer for AML purposes?

- 2.19 Identification of the parties associated with a card account is not dependent on whether or not they have a contractual relationship with the Card Issuer. A Card Issuer's contractual relationship is solely with the primary cardholder, whether that is a natural or legal person, and it is to the primary cardholder that the Issuer looks for repayment of the debt on the card. The primary cardholder is unquestionably the Issuer's customer. However, a number of secondary persons may have authorised access to the account on the primary cardholder's behalf, whether as additional cardholders on a personal account or as employees holding corporate cards, where the contractual liability lies with the corporate employer.
- 2.20 The question therefore arises as to the appropriate extent, if any, of due diligence to be undertaken in respect of such secondary cardholders. Hitherto, there have been marked variations in interpretation and practice between Card Issuers with regard to the amount of data collected on secondary cardholders and the extent to which it is verified.
- 2.21 In substance, an additional cardholder on a personal card account is arguably analogous to either a joint account holder of a bank account, but without joint and several liability attaching, or - perhaps more persuasively - to a third party mandate holder on a bank account. In the case of corporate cards, it is reasonable to take the position that verification of the company in accordance with the guidance in Part I does not routinely require verification of all the individuals associated therewith.
- 2.22 In both cases, the risk posed to a firm's reputation in having insufficient data to identify a secondary cardholder featuring on a sanctions list or being a corrupt politically exposed person, and the potential liability arising from a breach of sanctions or a major money laundering or terrorist financing case, renders it prudent for the data collected to be full enough to mitigate that risk.
- 2.23 A merchant is a customer for AML/CTF purposes of the Merchant Acquirer.

Customer due diligence

- 2.24 In most cases, the Card Issuer would undertake the appropriate customer due diligence checks itself, or through the services of a credit reference agency, but there are some exceptions to this:
- where the Card Issuer is issuing a card on behalf of another regulated financial services firm, being a company or partner (in the case of affinity cards) that has already carried out the required customer due diligence
 - introductions from other parts of the same group, or from other firms which are considered acceptable introducers (see Part I, section 5.6)
- 2.25 Although not an AML/CTF requirement, approval processes should have regard to the Card Issuer's latest information on current sources of fraud in relation to credit card applications.
- 2.26 Card schemes carry out surveys and reviews of activities related to their members. For example, one scheme carried out a due diligence review of the AML/CTF standards of all its members domiciled in high risk countries. Card Issuers should be aware of such survey/review activity.

FINAL BOARD APPROVED

- 2.27 Where corporate cards are issued to employees, the identity of the employer should be verified in accordance with the guidance set out in Part I, paragraph 5.3.112.
- 2.28 The standard verification requirement set out in Part I, Chapter 5 should be applied, as appropriate, to credit card and store card holders, although ascertaining the purpose of the account, and the expected flow of funds, would not be appropriate for such cards.
- 2.29 A risk-based approach to verifying the identity of secondary cardholders should be carried out as follows:
- The standard information set out in Part I, paragraph 5.3.59 should be collected for all secondary cardholders and recorded in such a way that the data are readily searchable.
 - Firms should assess the extent to which they should verify any of the data so obtained, in accordance with the guidance set out in Part I, paragraph 5.3.60, from independent documentary or electronic evidence, in the light of their aggregate controls designed to mitigate fraud and money laundering risks, and bearing in mind the extent to which the firm applies the risk controls set out in paragraph 2.18. However, there is a presumption that such verification will be carried out, other than in the following circumstances.
 - In the case of store cards, because of the restrictions on their use, see paragraph 2.6.
 - In the case of commercial cards, because of the restrictions on their issue, see paragraph 2.7, although a firm's risk-based approach may deem it prudent to verify employee cardholders of their smaller commercial card customers.

Where a firm employs a low risk strategy of issuing additional cards only to close family members who reside at the same address as the primary cardholder, and the additional cardholder is a close family member whose employment, or continuing education, dictates that they are not permanently resident at the address, then for purposes of verification the primary cardholder's address shall be the main residential address. This will be acceptable as long as the mailing address for the additional cardholder remains the same as the primary cardholder's address.

In all these situations, firms will still need to consider other types of due diligence check on additional cardholders, e.g., against sanctions lists.

- 2.30 In relation to branded and affinity cards, where another regulated firm has the primary relationship with the cardholder, the partner organisation would need to undertake that it holds information on the applicant, and that this information would be supplied to the card issuer if requested.
- 2.31 In respect of a merchant, the Merchant Acquirer should apply the standard verification requirement in Part I, Chapter 5, adjusted as necessary to take account of the activities in which the merchant is engaged, turnover levels, the sophistication of available monitoring tools to identify any fraudulent background history as well as transaction activity, and the location of the bank account over which transactions are settled.
- 2.32 Where functions in relation to card issuing, especially initial customer due diligence, is outsourced, the firm should have regard to the FCA's guidance on outsourcing (www.fsahandbook.info/FSA/html/handbook/SYSC/8). In particular, Card Issuers should have criteria in place for assessing, initially and on an ongoing basis, the extent and robustness of the systems and procedures (of the firm to which the function is outsourced) for carrying out customer identification.

FINAL BOARD APPROVED

- 2.33 It would be unusual for a Card Issuer to revisit the information held in respect of a cardholder. Credit cards are primarily a distance transaction process. An account is opened (after due diligence checks are completed), a balance is acquired, a bill sent and payment received. This cycle is repeated until card closure and the majority of cardholders rarely, if ever, contact the Card Issuer.

Enhanced due diligence

- 2.34 An issuer should have criteria and procedures in place for identifying higher risk customers. Such customers must be subject to enhanced due diligence. This applies in the case of customers identified as being PEPs, or who are resident in high-risk and/or non FATF jurisdictions.
- 2.35 Firms' procedures should include how customers should be dealt with, depending on the risk identified. Where necessary and appropriate, reference to a senior member of staff should be made in unusual circumstances. This will include getting senior manager approval for relationships with PEPs, although the level of seniority will depend on the level of risk represented by the PEP concerned.

Monitoring

- 2.36 It is a requirement of the ML Regulations that firms monitor accounts for unusual transactions patterns. Controls should be put in place for accepting changes of name or address for processing.

3: Electronic money

The purpose of this sectoral guidance is to provide clarification to electronic money issuers on customer due diligence and related measures required by law. As AML/CTF guidance, this sectoral guidance is incomplete on its own and must be read in conjunction with the main guidance set out in Part I and the specialist guidance set out in Part III.

This guidance may be used by all electronic money issuers (as defined in Regulation 2(1) of the Electronic Money Regulations 2011), including authorised electronic money institutions, registered small electronic money institutions, and credit institutions with a Part IV permission under the Financial Services and Markets Act 2000 to issue electronic money. It may also be relevant for EEA authorised electronic money issuers who distribute their products in the UK.

Introduction

What is electronic money?

- 3.1. Under the Electronic Money Regulations 2011 (Reg. 2(1)), electronic money is defined as:

‘electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which—

 - (a) is issued on receipt of funds for the purpose of making payment transactions;*
 - (b) is accepted by a person other than the electronic money issuer; and*
 - (c) is not excluded by regulation 3.’*
- 3.2. Regulation 3 of the Electronic Money Regulations 2011 states that electronic money does not include:

‘(a) monetary value stored on instruments that can be used to acquire goods or services only—

 - (i) in or on the electronic money issuer’s premises; or*
 - (ii) under a commercial agreement with the electronic money issuer, either within a limited network of service providers or for a limited range of goods or services;*

(b) monetary value that is used to make payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.’
- 3.3. Electronic money is therefore a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities. It may be a card-based, voucher-based, mobile app-based or an online account-based product.
- 3.4. The Electronic Money Regulations 2011 also provide for a number of exemptions (see para. 3.2 above). Where such products are exempted from financial services regulation, they are also likely to fall outside of the scope of the AML and CTF regulation. Issuers must, however, examine such products on a case-by-case basis to identify whether such regulation continues to apply.
- 3.5. Electronic money may be issued by banks or building societies with the requisite variation of permission from the FCA, or it may be issued by specialist electronic money institutions, who obtain an authorisation from the FCA under the Electronic Money Regulations 2011 (for other persons also permitted to issue electronic money, such as local authorities, see Regulation 2(1)

FINAL BOARD APPROVED

of the Electronic Money Regulations 2011.) Where electronic money institutions meet the conditions set out in Regulation 13 of the Electronic Money Regulations 2011, they may register with the FCA as small electronic money institutions.

- 3.6. All issuers of electronic money are subject to the Money Laundering Regulations 2017, the Terrorism Act 2000, the Anti-terrorism, Crime and Security Act 2001, the Wire Transfer Regulation, Schedule 7 to the Counter-terrorism Act 2008 and the Proceeds of Crime Act 2002. They must also comply with the legislation implementing the UK's financial sanctions regimes. Issuers of electronic money that are FSMA-authorised persons (i.e. banks and building societies) must also comply with relevant provisions in the FCA's handbook for AML/CTF purposes.
- 3.7. Electronic money may also be issued into the UK by EEA credit and financial institutions holding the appropriate passport from their home state competent authority under Art. 25 or 28 of the Banking Consolidation Directive (2006/48/EC) or Arts. 28 and 29 of the Payment Services Directive (EU) 2015/2366 by virtue of Art. 3(1) of the Electronic Money Directive (2009/110/EC). Where such issuance, distribution or redemption is on a cross-border services basis, i.e. without an establishment in the UK, the issuer's AML procedures are regulated by the home state authorities, but issuers must be aware that in some cases, UK legislation may extend to such providers of services. UK AML/CTF legislation will apply where the service is provided through an establishment in the UK.

Definitions

- 3.8. The following terms are used in this guidance:

- **Card-based products:**

These are products that employ a card for authentication. The electronic money will usually reside in an account on a server and not on the card itself.

- **Electronic Money Association (EMA):**

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers.

- **Merchant:**

For the purposes of this guidance, a merchant is a natural or legal person that uses electronic money to transact in the course of business. Where an electronic money issuer is part of a four-party scheme, the issuer might not have a direct business relationship with all merchants.

- **Mobile app-based products:**

These products provide access to account-based e-money which will usually reside on a remote server.

- **Online account-based products:**

These are products where the value held by a customer is held centrally on a server under the control of the issuer. Customers access their purses remotely.

- **Payment Service Provider (PSP):**

PSPs are defined in Article 3(5) of the Wire Transfer Regulation as being inclusive of credit institutions, e-money institutions (full and small) and payment institutions (full and small) that provide transfer of funds services.

- **Purse:**

An electronic money purse is a store of electronic money, usually in the form of an account.

FINAL BOARD APPROVED

- **Redemption:**

This is the process whereby a customer presents electronic money to the issuer and receives its monetary value in exchange at par. (Note that the term is also sometimes used in the gift card industry to indicate the spending of value with merchants. This meaning is not intended here.)

- **Three- and four-party schemes:**

An electronic money system can comprise a single issuer that contracts with both consumer and merchant, or it can be made up of a number of issuers and acquirers, each issuer having its own consumer base, each acquirer its own merchant base. The former is referred to as a three-party scheme, comprising issuer, consumer and merchant, whereas the latter is known as a four-party scheme, comprising issuer, acquirer, consumer and merchant.

- **Voucher-based products:**

Some electronic money products are issued as electronic vouchers of a fixed value that can only be spent once. Any value that remains on the voucher can either be redeemed, or a new voucher issued. The value associated with a voucher is usually held centrally on a server.

- **Wire Transfer Regulation (WTR):**

Regulation (EU) 2015/847 on information accompanying transfers of funds implements FATF Recommendation 16 on wire transfers in EEA member states. This guidance refers to it as the Wire Transfer Regulation, although this term has no formal standing.

Notes

- 3.9. The cumulative turnover limit of an electronic money purse is interpreted as the total amount of electronic money received by a purse during a period of time, whether through the purchase of electronic money or the receipt of electronic money from other persons.

Money laundering and terrorist financing risks related to electronic money

- 3.10. Electronic money is a retail payment product that is used predominantly for making small value payments. It is susceptible to the same risks of money laundering and terrorist financing as other retail payment products. In the absence of AML systems and controls, there is a significant risk of money laundering taking place. The implementation of AML systems and controls and certain product design features can contribute to mitigating this risk.
- 3.11. Furthermore, where electronic money is limited to small value payments, its use is less attractive to would-be launderers. For terrorist financing and other financial crime, electronic money offers a more accountable, and therefore less attractive means of transferring money compared to cash.
- 3.12. The electronic money products in commercial use today do not provide the privacy or anonymity of cash, nor its utility. This is due to a number of factors. Products may, for example, be funded by payments from bank accounts or credit cards and therefore reveal the identity of the customer at the outset. The use of most electronic money products leaves an electronic trail that can help locate, if not identify, the user of a particular product.
- 3.13. As issuers of electronic money usually occupy the position of intermediaries in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement that complements identity data provided by other financial institutions. This may be equally or more valuable evidence than a repetition of the verification of identity process.

FINAL BOARD APPROVED

- 3.14. Fraud prevention and consumer protection concerns lead to the placement of transaction, turnover and purse limits on products, limiting the risk to both issuer and consumer. These limits act to restrict the usefulness of the product for money laundering, and make unusual transactions more detectable.
- 3.15. A non-exhaustive list of risk factors that may apply to electronic money products is given in para. 3.18 below; risk mitigating factors are listed in para. 3.20 below. Other risks set out in the draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities and in Part I, Annex 4-II of this guidance also affect issuers, and issuers should consider these as part of the risk assessment that they undertake. Issuers should in particular be alert to emerging information on financial crime risks specific to electronic money, such as those highlighted by
- Their own transaction monitoring processes;
 - The FCA;
 - The NCA;
 - National and supra-national risk assessments and associated recommendations;
 - The Joint Committee of the European Supervisory Authorities;
 - The European Commission (EC list of high-risk third countries); and
 - Typology reports, such as those from the EMA and the FATF.
- 3.16. The overall ML/TF risk posed by an electronic money product is a function of its design, its use, and the issuer's AML/CTF controls. The overall risk posed is the outcome of competing factors, not any single feature of the product.¹
- 3.17. Issuers will need to put in place risk management processes appropriate to the size and nature of their business and must evidence that they deploy an adequate range of controls to mitigate the ML/TF risks they encounter.

Risk factors

- 3.18. The following factors will increase the risk of electronic money products being used for money laundering or terrorist financing (for ways in which this risk can be mitigated by applying controls or by other means, see para. 3.21 below):
- High transaction or purse limits, particularly where compared to anticipated usage, or where customers are permitted to hold multiple purses; The ability to conduct cross-border transactions, although the risk may be less within 3-party schemes that afford the issuer oversight over both payer and payee;
 - E-money issuers can use complex business models such as using programme managers to 'white label' their products, this can result in a complex control environment and therefore in a higher risk that a particular product could be used for ML/TF;
 - Some merchant activity, such as betting and gaming, poses a higher risk of money laundering. This is because of the higher amounts of funds that are transacted and because of the opportunities presented within the merchant environment;

¹ The draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities, paras. 31-32, state: "Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of money laundering and terrorist financing risk associated with a business relationship or occasional transaction. As part of this assessment, firms may decide to weigh factors differently depending on their relative importance."

FINAL BOARD APPROVED

- Funding of purses by unverified parties presents a higher risk of money laundering, whether it is the customer who is unverified or a third party;
 - Funding of purses using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering²;
 - Funding of purses using electronic money products that have not been verified may present a higher risk of money laundering³;
 - The non-face-to-face nature of many products gives rise to increased risk;
 - The ability of consumers to hold multiple purses (for example open multiple accounts or purchase a number of cards) without verification of identity increases the risk;
 - Cash access, for example by way of ATMs, as well as an allowance for the payment of refunds in cash for purchases made using electronic money, will increase the risk⁴;
 - Increased product functionality may in some instances give rise to higher risk of money laundering (product functionality includes person-to-business, person-to-person, and business-to-business transfers);
 - Products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the customer is able to pass on linked ‘partner’ cards to anonymous third parties;
 - Segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk;
 - The technology adopted by the product may give rise to specific risks that should be assessed.
- 3.19. Absence of any of the above factors will decrease the risk.

Risk mitigating factors

- 3.20. Electronic money issuers address the risks that are inherent in payments in a similar manner to other retail payment products by putting in place systems and controls that prevent money laundering and terrorist financing by detecting unusual transactions and predetermined patterns of activity.
- 3.21. The systems and controls issuers put in place must be commensurate to the money laundering and terrorist financing risk they are exposed to. The detail of issuers’ systems and controls will therefore vary. Examples include those that:
- Strong oversight of outsourced functions;
 - Place limits on purse storage values, cumulative turnover or amounts transacted;
 - Can detect money laundering transaction patterns, including those described in the EMA or similar typologies documents;
 - Will detect anomalies to normal transaction patterns;
 - Can identify multiple purses held by a single individual or group of individuals, such as the holding of multiple accounts or the ‘stockpiling’ of pre-paid cards;

² For transfers subject to the Regulation, see the requirements for up-front verification where transfers are funded by cash or electronic money in Article 5(3)(a)

³ For transfers subject to the Regulation, see the requirements for up-front verification where transfers are funded by cash or electronic money in Article 5(3)(a)

⁴ For transfers subject to the Regulation, see the requirements for up-front verification where transfers are paid out in cash or electronic money in Article 7(4)(a)

FINAL BOARD APPROVED

- Can look for indicators of accounts being opened with different issuers as well as attempts to pool funds from different sources;
- Can identify discrepancies between submitted and detected information, for example, between country of origin submitted information and the electronically-detected IP address, geo-location information or device-related information;
- Deploy sufficient resources to address money laundering risks, including, where necessary, specialist expertise for the detection of suspicious activity;
- Allow collaboration with merchants that accept electronic money to identify and prevent suspicious activity;
- Restrict funding of electronic money products to funds drawn on accounts held at credit and financial institutions in the UK, the EU or a comparable jurisdiction, and allow redemption of electronic money only into accounts held at such institutions.

Customer Due Diligence

- 3.22. The Money Laundering Regulations 2017 require firms to apply customer due diligence measures on a risk-sensitive basis. Customer due diligence measures comprise the identification and verification of the customer's (and, where applicable, the beneficial owner's) identity and obtaining information on the purpose and intended nature of the business relationship or transaction. There is also a requirement for the ongoing monitoring of the business relationship. Part I, Chapter 5 sets out how firms can meet these requirements.
- 3.23. Detailed guidance for verifying the identity of customers who do not have access to a bank account, or who lack credit or financial history, is provided under the financial exclusion provisions of Part I, paras. 5.3.108 to 5.3.125.
- 3.24. Issuers will also need to satisfy themselves that they comply with sanctions legislation. Guidance on this is provided throughout Part I and in Part III, section 4.

Verification of identity – consumers

- 3.25. Taking account of the risk mitigation features applied to electronic money systems, the approach to undertaking customer due diligence in the electronic money sector is predicated on the need to minimise barriers to take-up of the products, whilst addressing the risk of money laundering and meeting the obligations set out in the Money Laundering Regulations 2017.
- 3.26. In addition to normal customer due diligence, the Money Laundering Regulations 2017 specify the following exemptions and allowances in relation to customer due diligence:
- **The e-money-specific exemption:** Circumstances where an exemption from the requirement to apply customer due diligence measures may be applied. A purse must meet specific functionality, storage, turnover and redemption restrictions in order to qualify for the e-money-specific exemption (see paras. 3.30 to 3.34 below), and issuers must have systems and controls in place to make sure these restrictions are not breached.
 - **Simplified due diligence:** Circumstances where simplified due diligence may be applied. The allowance to apply simplified due diligence is risk-based, and parameters will differ between products. Where the product is no longer low risk, where the issuer doubts the veracity or accuracy of documents or information previously obtained, or where the issuer suspects money laundering or terrorist financing, customer due diligence and, where appropriate, enhanced due diligence measures must be applied.

FINAL BOARD APPROVED

- 3.27. Monitoring of the business relationship and transactions must be undertaken during the application of both the e-money-specific exemption and simplified due diligence. Issuers should also comply with the requirements set out in paras. 3.46 to 3.49 below.
- 3.28. Issuers, in common with other financial services providers, are required to verify identity of the customer at the outset of a business relationship. The e-money-specific exemption and simplified due diligence enable issuers to postpone the verification of identity until the exemption limits have been reached. Issuers making use of these provisions whose electronic money products may at some point exceed these limits should have in place systems to anticipate when a customer approaches the exemption limits. Where there is an obligation to undertake customer due diligence and this cannot be discharged, issuers must freeze the account pending the provision of the required information.
- 3.29. Enhanced due diligence is required in circumstances giving rise to an overall higher risk. The extent of enhanced due diligence measures required will depend on the level of risk a situation presents (see paras. 3.50 to 3.53 below).

The e-money-specific exemption

- 3.30. The Money Laundering Regulations 2017 (Reg. 38(1) and (2)) set limits for reloadable and non-reloadable electronic money products, above which customer due diligence measures must be applied:

(1) Subject to paragraph (3), a relevant person is not required to apply customer due diligence measures in relation to electronic money, and regulations 27, 28, 30 and 33 to 37 do not apply provided that—

- (a) the maximum amount which can be stored electronically is 250 euros or (if the amount stored can only be used within the United Kingdom), 500 euros;*
- (b) the payment instrument used in connection with the electronic money (“the relevant payment instrument”) is—*
 - i) not reloadable, or*
 - ii) is subject to a maximum limit on monthly payment transactions of 250 euros which can only be used in the United Kingdom;*
- (c) the relevant payment instrument is used exclusively to purchase goods or services;*
- (d) anonymous electronic money cannot be used to fund the relevant payment instrument.*

(2) Paragraph (1) does not apply to any transaction which consists of the redemption in cash, or a cash withdrawal, of the monetary value of the electronic money, where the amount redeemed exceeds 100 euros.

(3) The issuer of the relevant payment instrument must carry out sufficient monitoring of its business relationship with the users of electronic money and of transactions made using the relevant payment instrument to enable it to detect any unusual or suspicious transactions.

(4) A relevant person is not prevented from applying simplified customer due diligence measures in relation to electronic money because the conditions set out in paragraph (1) are not satisfied, provided that such measures are permitted under regulation 37.

(5) For the purposes of this regulation “payment instrument” has the meaning given by regulation 2(1) of the Electronic Money Regulations 2011(a).

Non-reloadable purses

FINAL BOARD APPROVED

- 3.31. Electronic money purses that cannot be recharged may benefit from the e-money-specific exemption if:
- The purse limit is restricted to €250 (or €500 if the amount stored can only be used within the United Kingdom);
 - The instrument is used only for purchase transactions of goods and services;
 - The device cannot be funded with anonymous e-money; and
 - The customer does not seek to redeem more than €100 in cash in a single transaction and the cash withdrawal does not cause the purse limit to be exceeded.
- 3.32. Non-reloadable purses are often sold as gift cards. The purchase of multiple such products is sometimes expected, particularly during certain times of the year, and the risk of money laundering arising from multiple purchases is likely to remain low. Issuers should, however, adopt a maximum total value that they will allow single customers to purchase without carrying out customer due diligence measures. This total value can be determined on a risk weighted basis, but should not exceed €1,500.

Reloadable purses

- 3.33. Electronic money purses that can be recharged may benefit from the e-money specific exemption if:
- The purse limit is restricted to €500 ;
 - The monthly turnover is restricted to €250;
 - The instrument is restricted to use within the United Kingdom;
 - The instrument is used only for purchases of goods and services;
 - The device cannot be funded with anonymous e-money; and
 - The customer does not seek to redeem more than €100 in cash in a single transaction and the cash withdrawal does not cause the monthly turnover limit to be exceeded.

Simplified due diligence

- 3.34. Issuers may apply simplified due diligence measures in addition to the limits set by the e-money-specific exemption if business relationships or transactions present a low risk of money laundering or terrorist financing.
- 3.35. The assessment of low risk is based on the risk factors set out in Regulation 37(3) and 37(4)..
- 3.36. Simplified due diligence must always involve the identification and verification of the customer, but the extent of identification and verification can be varied depending on the risk, and verification may be postponed⁵ until the risk is no longer deemed to be low. In this case, issuers should set a reasonable threshold that will minimise potential abuse of the product.
- 3.37. Simplified due diligence may also involve verifying identity on the basis of fewer or less reliable sources, using alternative methods to verify identity, assuming the nature and intended purpose of the business relationship where this is obvious or reducing the intensity of monitoring.

⁵ See the draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities, paragraph 124. Also see Part I, Annex 5-III.

FINAL BOARD APPROVED

Verification by reliance on the funding instrument under simplified due diligence

- 3.38. As part of a risk-based approach to verification of identity, the Money Laundering Regulations 2017 require that verification is carried out “on the basis of documents or information obtained from a reliable source which is independent of the customer.” In some cases, where the risk associated with the business relationship is low, a customer’s funding instrument (such as a credit card or bank account) can constitute such information, subject to the following additional requirements:
- a) The issuer remains ultimately responsible for meeting its customer due diligence obligations;
 - b) The issuer has in place systems and processes for identifying incidents of fraudulent use of credit/debit cards and bank accounts;
 - c) The issuer has in place systems and processes that enable monitoring to identify increased risk for such products. If the risk profile can then no longer be regarded as low risk, additional verification steps must be undertaken;
 - d) The issuer records and keeps records of relevant information, for example IP addresses, which assist in determining the electronic footprint of the customer, or where a POS terminal is used in a face-to-face environment, records the correct use of a PIN or other data;
 - e) The funds to purchase electronic money are drawn from an account or credit card with, or issued by, a credit or financial institution⁶ in the UK, the EU or an equivalent jurisdiction, which is supervised for its AML controls;
 - f) The issuer implements systems and controls to mitigate the risk of the funding card or account being itself subject to SDD;
 - g) The issuer has reasonable evidence to conclude that the customer is the rightful holder of the account on which the funds are drawn (which may be achieved using the processes described in para. 3.41 below);
- 3.39. A funding instrument on its own, however, is a weak form of verification of identity. The credit or financial institution whose evidence is being used may not have verified the customer to current standards, and there is a risk that the person using the account is not its rightful holder. This risk is even higher where an electronic money issuer has no evidence that the account is held in the same name as the customer, as is the case, for example, in relation to direct debits.

Establishing control over the funding instrument

- 3.40. Where payment is made electronically, it is usually not possible to verify the name of the account holder for the funding account. In this case, steps must be taken to establish that the customer is the rightful holder of the account from which the funds are drawn. These steps may include the following:
- Micro-deposit. Some issuers have developed a means of establishing control over a funding account using a process that is convenient and effective. A small random amount of money is credited to a customer’s funding account and the customer is then required to discover the amount and to enter it on the issuer’s website. By entering the correct value, the customer demonstrates access to the bank/card statement or accounting system of their bank or financial institution. This method, and its close variants (such as the use of unique reference numbers), provides an acceptable means of confirming that the customer has access to the account, and therefore has control over it. It also provides a means of guarding

⁶ Other than a money service business, or a payment or electronic money institution providing mainly money remittance services.

FINAL BOARD APPROVED

against identity theft, contributing therefore to the verification of identity process. If such an approach is not used, some other means of establishing control of the account is needed.

- Additional fraud checks. Issuers may also use additional fraud checks undertaken at the time of the transaction which seek to cross reference customer-submitted data against data held by the electronic money or card issuer or similar independent third party, and which gives the electronic money issuer the requisite level of confidence that the customer is the rightful holder of the card.
 - Evidence of legitimate use. Seeking evidence of legitimate use is an alternative to establishing formal control over an account. An account that is used to fund an electronic money purse over a significant period of time is more likely to be used legitimately, as the passage of time gives the rightful owner the opportunity to discover fraudulent use of the product and to block its use, which would in turn become evident to the issuer. Thus, for some products, this may provide a means of establishing legitimate use of a funding instrument. However:
 - Such an approach is sensitive to the issuer's ability to monitor, track and record use of a funding instrument associated with an account, and issuers wishing to adopt this approach must therefore have systems that are appropriate for this purpose.
 - A minimum period of four months must elapse, together with significant usage in terms of number and value of transactions over this time, to satisfy the issuer that the instrument is being legitimately used.⁷
- 3.41. Electronic money issuers must have processes in place to ensure that additional due diligence measures are applied if the money laundering and terrorist financing risk posed by the product or customer increases.
- 3.42. Information on the payer that is received as part of the obligations under the WTR may contribute to verifying a customer's identity.

Basic requirements under this guidance in relation to products benefiting from the e-money-specific exemption and those applying simplified due diligence

- 3.43. This guidance provides for additional measures in relation to the application of simplified due diligence. Issuers should adopt the following measures that relate to verification of identity and monitoring:

Verification of identity

- 3.44. Either the electronic money system is a 3-party scheme; or
- It is a 4-party scheme, in which case all other participating issuers should under this guidance meet the following requirements:
- a) In all cases merchants must be subject to due diligence measures in accordance with Part I, Chapter 5 (but see para. 3.60 below for a limited exemption) or as required by an equivalent jurisdiction.
 - b) Where electronic money is accepted by merchants or other recipients belonging to a wider payment scheme (for example Visa or MasterCard), issuers must satisfy themselves that the verification of identity and other due diligence measures carried out by that scheme in relation to merchants are, in the UK, equivalent to those of this sectoral guidance; or for other jurisdictions, are subject to equivalent requirements.

⁷ The four-month period should be completed before any limits associated with simplified due diligence are exceeded.

FINAL BOARD APPROVED

- c) Where redemption of electronic money is permitted by way of cash access, for example through withdrawal at ATMs or through a cash-back facility at retailers, and where controls cannot be implemented to prevent this exceeding the cash redemption limit under the e-money-specific exemption or any other cash redemption limit associated with simplified due diligence, customer due diligence must be carried out at the point of issuance of the electronic money or before such functionality is enabled. Furthermore, issuers must, wherever possible, require all refunds made by merchants in the event of return of goods or services to be made back onto the electronic money purse from which payment was first made.

Monitoring

- 3.45. Issuers must establish and maintain appropriate and risk-sensitive policies and procedures to monitor business relationships and transactions on an ongoing basis. Part I Chapter 5 (see in particular section 5.7) sets out how this can be done.
- 3.46. If issuers wish to benefit from the e-money-specific exemption or the simplified due diligence provisions under this guidance, they must, in addition to the processes set out in part I Chapter 5, deploy specific minimum transaction monitoring and/or on-chip purse controls that enable control of the systems and recognition of suspicious activity. Such controls may include:
- Transaction monitoring systems that detect anomalies or patterns of behaviour, or the unexpected use of the product, for example frequent cross-border transactions or withdrawals in products that were not designed for that purpose;
 - Systems that identify discrepancies between submitted and detected information – for example, between submitted country of origin information and the electronically-detected IP address;
 - Systems that cross-reference submitted data against existing data for other accounts, such as the use of the same credit card or device by several customers;
 - Systems that interface with third party data sources to import information that may assist in detecting incidence of fraud or money laundering across a number of payment service providers;
 - On-chip controls that impose purse rules, such as those specifying the POS terminals or other cards with which the purse may transact;
 - On-chip controls that impose purse limits such as transaction or turnover limits;
 - On-chip controls that disable the card when a given pattern of activity is detected, requiring interaction with the issuer before it can be re-enabled;
 - Controls that are designed to detect and forestall the use of the electronic money product for money laundering or terrorist financing in accordance with the typologies identified for such a product.
- 3.47. Information obtained through monitoring must be reviewed as part of the ongoing risk assessment; issuers must apply customer due diligence measures and monitoring appropriate to the risks.
- 3.48. Issuers are reminded that in the event that potentially suspicious activity is detected by internal systems or procedures, they must must comply with their obligations under POCA and the Terrorism Act 2000 (see Part I, Chapter 6) to report possible money laundering or terrorist financing.

FINAL BOARD APPROVED

Enhanced due diligence

- 3.49. The Money Laundering Regulations 2017 require enhanced due diligence to be undertaken in all situations where the risk of money laundering is perceived to be high. These include instances where the customer is not physically present for identification purposes,⁸ as well as in respect of business relationships or occasional transactions with politically exposed persons (PEPs)⁹.
- 3.50. Where electronic money purses are purchased or accounts opened in a non-face-to-face environment, issuers must take specific and adequate measures to address the greater risk of money laundering or terrorist financing that is posed (see Part I, paras. 5.3.85 to 5.3.91 on the mitigation of impersonation risk arising from non-face-to-face transactions). Issuers may adopt means of verification other than those outlined in Part I, provided that these are commensurate to the risk associated with the business relationship.
- 3.51. The requirement for issuers to have systems and processes to detect PEPs will be proportionate to the risk posed by the business relationship, as will the degree of enhanced due diligence required for PEPs. Issuers should focus their resources in a risk sensitive manner on products and transactions where the risk of money laundering is high. Further guidance on the application of the risk-based approach to PEPs is provided in Part I, paras. 5.5.24 to 5.5.28.
- 3.52. In all other high risk scenarios, issuers should have regard to the guidance in Part I Chapter 5.

Multiple-card products

- 3.53. Issuers whose products enable two or more cards to be linked to a single account must establish whether they have entered into one or more business relationships, and must verify the identity of all customers with whom they have a business relationship.
- 3.54. Issuers should also consider whether the functionality of the second card may give rise to beneficial ownership.
- 3.55. Issuers should consider undertaking CDD even in the absence of a business relationship with, or beneficial ownership by, additional card holders on a risk-based approach. Where additional card holders remain non-verified, issuers must nevertheless implement controls to mitigate the greater risk of money laundering and terrorist financing to which these products are exposed.

Verification of identity – merchants

- 3.56. The FCA expects electronic money issuers to understand who their merchants are in order to guard against the risk that their electronic money products might be used for money-laundering or terrorist financing.
- 3.57. Issuers must therefore apply ongoing due diligence to merchants on a risk-sensitive basis in accordance with Part I, Chapter 5. This includes the requirement to undertake adequate due diligence on the nature of the merchant's business and to monitor the relationship.
- 3.58. In person-to-person systems, the boundary between consumers and merchants may be blurred; consumers may not register as merchants, but may nevertheless carry on quasi-merchant activity. In this case issuers:

⁸ But note that if an electronic money purse meets the conditions for the e-money-specific exemption, no identification of the customer is required, even though the customer may not have been physically present. Outside the conditions for the e-money-specific exemption, this risk factor is merely one of many and may be mitigated against, see para. 3.16 above.

⁹ If an electronic money purse meets the conditions for the e-money specific exemption, no PEP-related processes are required, even though the customer may be a PEP.

FINAL BOARD APPROVED

- Should have systems in place that provide a means of detecting such activity.
 - When such activity has been detected, apply due diligence measures appropriate to merchants.
- 3.59. Issuers may allow merchants to benefit from the €250 monthly turnover and €100 redemption allowance in order to enable the online recruitment of small merchants. This does not, however, alter the requirement to undertake adequate due diligence on the nature of the merchant's business.

Wire Transfer Regulation

- 3.60. Guidance on the requirements of the WTR is provided in Part I, paras. 5.2.10 to 5.2.13 and in Part III, Specialist Guidance 1: *Wire transfers*.

Scope

- 3.61. Issuers may be subject to the requirements of the WTR in their role as PSP of the payer, PSP of the payee or intermediary PSP.
- 3.62. Only those issuers that offer products that are used for person-to-person transfers or where the number of the e-money instrument does not accompany all transfers flowing from the transaction are subject to the requirements of the WTR.
- 3.63. Where an electronic money purse is funded through a card payment, this funding transaction is a payment for goods and services and is therefore out of scope according to Article 2(3) of the WTR (also see Part III, para. 1.17).

Verification requirements under the WTR

- 3.64. Verification of information under the WTR should be undertaken using a risk-based approach as provided for elsewhere in this guidance or as set out in Part III.
- 3.65. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payer by the PSP of the payer unless the funds are received in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.
- 3.66. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payee by the PSP of the payee unless the funds are paid out in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.

Redemption of electronic money

- 3.67. Payments made to customers in redemption of electronic money are usually made by bank transfer. Redemption comprises a payment by the issuer as principal (payer) to the electronic money account holder (payee). Issuers may, however, attach customer (in addition to their own) information as information on the payer to the redemption transaction in the usual way – benefitting from the provisions for inter EU payments where applicable, and ensuring additional information is available to the payee PSP.
- 3.68. Where redemption is made in cash, this benefits from the exemption from the WTR for cash withdrawals from a customer's own account under Article 2(4)(a).

FINAL BOARD APPROVED

Use of agents and distributors

- 3.69. Issuers may distribute or redeem electronic money through an electronic money distributor or can offer payment services through a payment services agent. Payment services agents must be registered with the FCA. Issuers are ultimately responsible for compliance with AML-related obligations where these are outsourced to their distributors and payment services agents. Issuers must be aware of the risk of non-compliance by their outsourced service providers and should take risk-based steps to monitoring the extent to which outsourced services are complying with their AML/CFT policies.
- 3.70. Issuers should apply the same customer due diligence measures to distributors as they do to merchants.
- 3.71. The FCA expects issuers to carry out fitness and propriety checks on payment services agents of electronic money issuers. These checks should include, among others, the assessment of the agents' honesty, integrity and reputation in line with Chapter 3 of the FCA's electronic money approach document.
- 3.72. Issuers are required to supply the FCA with a description of the internal control mechanisms their payment services agents have in place to comply with the Money Laundering Regulations 2017 and the Proceeds of Crime Act 2002. Where the payment services agent is established in another EEA jurisdiction, the issuer must ensure their AML systems and controls comply with local legislation and regulation that implements the 4th Money Laundering Directive. Issuers must also take reasonable measures to satisfy themselves that their payment services agents' AML/CTF controls remain appropriate throughout the agency relationship.

Central contact points

- 3.73. Depending on their activities, when distributors or payment services agents are used to passport services to another EEA jurisdiction, these may be regarded as establishments in a form other than a branch and some member states may require issuers to establish a central contact point on their territory. The Joint Committee of the European Supervisory Authorities is developing regulatory technical standards for central contact points and these should be referred to when establishing and overseeing contact points.
- 3.74. Regulation 22 of the Money Laundering Regulations 2017 gives the FCA the power to request electronic money issuers to appoint a person to act as a Central Contact Point in the UK if they are established in the UK in a form other than a branch and have their head office in an EEA state, on any issue relating to the prevention of money laundering or terrorist financing.
- 3.75. What amounts to an establishment is defined in the Treaty, and guidance on the meaning of establishment has been issued by the European Commission in 1997.¹⁰

4: Credit unions

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance. This guidance covers aspects of money laundering compliance that are unique to credit unions and an overview of the key compliance issues; credit unions must also take account of Part I of this guidance.

Credit unions will also need to be aware of SYSC 6.3.

Overview of the sector

- 4.1. The membership of a credit union is restricted to individuals who fulfil a specific qualification which is appropriate to a credit union (and as a consequence a common bond exists between members) - Credit Unions Act 1979, s1(2)(b). The common bond concept is central to the co-operative ethos of a credit union and is also fundamental to the regulatory regime for credit unions.
- 4.2. The FCA has produced additional common bond guidance outlining geographical and population limits regarding common bonds.
- 4.3. Credit unions therefore operate within a restricted, often localised market, providing services to members, not to the public at large.

What are the money laundering and terrorist financing risks in credit unions?

- 4.4. The majority of credit unions offer very basic savings and loan products, although some offer more flexibility around the products they can provide. Overall, however, credit unions are restricted in terms of the range and complexity of the products they can offer and to whom they can offer them.
- 4.5. There are limits on the level of savings a credit union can hold on behalf of an individual member, which are set out in CREDS 4.2 and Section 2 of the Credit Union Part, PRA Rulebook. The return on savings is linked to financial performance. In addition, there are rules governing a credit union's lending activity. Lending limits are set out in CREDS 7.3 and Section 3 of the Credit Union Part, PRA Rulebook.
- 4.6. Therefore credit union financial products do not deliver sufficient functionality or flexibility to be the first choice for money launderers, although these restrictions may not be such a deterrent to terrorist financiers.
- 4.7. The high levels of cash transactions going through credit unions may be one area where there is a higher risk of money laundering or terrorist financing, e.g., by 'smurfing'¹¹.

¹¹ Numerous small payments into an account, where the amount of each deposit is unremarkable but the total of all the credits is significant.

FINAL BOARD APPROVED

- 4.8. The number of staff and volunteers involved in the day to day operations of a credit union is relatively small and, even in larger credit unions, there are typically no more than a few individuals whose responsibility it is to manually process data. Therefore, where there is manual processing of all transactions, the ability to identify suspicious transactions is potentially much greater. In addition, the relatively small organisational structures mean that suspected money laundering or terrorist financing can be detected and reported much faster in smaller credit unions than it could in other financial services firms. The monitoring procedures for larger credit unions, that inevitably do not have such a close relationship with their members, will need to reflect the absence of those relationships, to ensure that potential problems, e.g., ‘smurfing’, can be detected.
- 4.9. This does not, of course, mean that there is no risk of money laundering or terrorist financing in credit unions and credit unions must in any case be aware of their responsibilities under the ML Regulations, the Proceeds of Crime Act (POCA) and the Terrorism Act. Credit unions must therefore establish appropriate procedures to monitor activities, with a particular scrutiny of those that carry a higher risk of money laundering or terrorist financing (see Part I, section 5.7). Examples of such activities include:
- money transfers to third parties;
 - large one off transactions;
 - third parties paying in cash on behalf of the member;
 - unusual loan or saving transactions;
 - reluctance to provide documentary evidence of identity when opening an account (even when taking into account financial exclusion issues).

Applying a risk-based approach

- 4.10. In accordance with the guidance in Part I, Chapter 4, a credit union’s risk-based approach will ensure that its strategies are focused on deterring, detecting and disclosing in the areas of greatest perceived vulnerability. The credit union needs to take a number of steps, documented in a formal policy statement which assesses the most effectual, cost effective and proportionate way to manage money laundering and terrorist financing risks. These steps are:
- identify the money laundering and terrorist financing risks that are relevant to the firm;
 - assess the risks presented by the credit union’s particular
 - Members;
 - Products;
 - Delivery channels;
 - Geographical areas of operation;
 - design and implement controls to manage and mitigate these assessed risks;
 - monitor and improve the effective operation of these controls; and
 - record appropriately what has been done and why.
- 4.11. A credit union will need to take account of its own experience and knowledge of its members and their financial activities. Credit unions should also consult the Financial Action Task Force website at www.fatf-gafi.org in order to keep up-to-date with money laundering/terrorist financing typologies.
- 4.12. Following the establishment of a risk-based approach, it is the responsibility of the credit union’s senior management to keep this strategy under regular review. Credit unions may consider it appropriate to have a standing item covering money laundering on the agenda of their monthly meeting to ensure procedures are being regularly reviewed. Credit unions will also need to take into account SYSC 6.3.8 which reads, “a firm must allocate to a director or senior manager (who may also be the money laundering reporting officer) overall responsibility

FINAL BOARD APPROVED

within the firm for the establishment and maintenance of effective anti-money laundering systems and controls”.

Customer due diligence

- 4.13. The anti-money laundering (AML)/combating the financing of terrorism (CTF) checks carried out during account opening are one of the primary controls for preventing criminals opening an account and are therefore an important element of AML/CTF procedures. Credit unions should be satisfied that the policies and procedures in place for verifying identity are effective in preventing and detecting money launderers and that they make provision for circumstances when increased evidence is required.
- 4.14. For the majority of members, the standard identification requirement set out in Part I, Chapter 5 (full name, residential address and date of birth) including, in the case of customers not met face to face, consideration of the additional precautions set out in Part I, paragraphs 5.3.85 – 5.3.90. Where relevant, obtaining the additional customer information set out in Part I, section 5.5, will be applicable.
- 4.15. The identity information should be verified in accordance with the guidance set out in Part I (paragraphs 5.3.72-5.3.84), either from documents produced by the individual, or electronically, or through a combination of the two: these approaches are potentially equal options, depending on the circumstances in any given case.

Documentary verification

- 4.16. Examples of documents that are acceptable in different situations are summarised in Part I, paragraph 5.3.76, together with the principles defining when reliance may be placed on a single document or where more than one is required. A current UK passport or photocard driving licence issued in the UK should be the document used in the majority of cases, other than in individual cases of financial exclusion, where it is concluded that an individual cannot reasonably be expected to provide standard identification, (see paragraphs 4.18-4.20 for further information). For non-UK residents, a national passport or national identity card is likely to be used in the majority of cases. However, in circumstances where the individual cannot be expected to produce standard identification credit unions can follow the guidance on financial exclusion in paragraphs 4.18-4.20.

Electronic verification

- 4.17. Electronic verification may be used to meet a firm’s customer identification obligations. However, a credit union should first consider whether electronic verification is suitable for its membership base, and should then have regard to the guidance in Part I, paragraphs 5.3.52-5.3.53 and 5.3.79–5.3.84. When using electronically-sourced evidence to verify identity, credit unions should ensure that they have an adequate understanding of the data sources relied on by the external agencies that supply the evidence. Credit unions should be satisfied that these sources provide enough cumulative evidence to provide reasonable certainty of a person’s identity, and conform with the guidance set out in Part I, Chapter 5. An electronic check that accesses a single database (e.g., Electoral Register check) is normally not enough on its own to verify identity.

Financial exclusion

- 4.18. 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

FINAL BOARD APPROVED

sense; for example, the Financial Inclusion Commission 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 believe that they will be refused.

- 4.19. As a first step, before concluding that a member cannot produce evidence of identity, credit unions will have established that the guidance on initial identity checks for personal customers set out in Part I, paragraphs 5.3.72-5.3.84 cannot reasonably be applied. Where the credit union has concluded that a member cannot reasonably be expected to meet the standard identification requirements, the guidance in Part I, paragraphs 5.3.115–5.3.116 should be followed. Where the alternative evidence set out in sector 1: *Retail banking*, Annex 1-I cannot be applied, a letter or statement from an appropriate person¹² who knows the individual, that indicates that the person is who he says he is, can be accepted as evidence of identity.
- 4.20. Where a credit union has concluded that it should treat a member as financially excluded, a record should be kept of the reasons for doing so.

Employee credit unions

- 4.21. Roughly ten percent of British credit unions are employee credit unions, but they represent a significant proportion of the overall assets and membership of the movement. All members of employee credit unions share the common bond of being associated with one particular employer or employer group, which must be large enough to provide enough members to sustain a viable credit union. The most common examples of employee credit unions are local authority, police and transport credit unions.
- 4.22. Employee credit unions should also have their own standard identity verification requirements to ensure that the member is indeed an employee (e.g., wage slip, employee identity card, other documented knowledge that the credit union has) and have therefore undertaken the appropriate identity checks. It should be noted that these checks are for the purpose of satisfying the common bond qualification for membership, as opposed to being for AML/CTF purposes.
- 4.23. To satisfy the requirements of AML/CTF legislation, additional identity verification checks should be sought, as described in paragraphs 4.15–4.17 of this chapter.
- 4.24. Employee credit unions whose common bond extends to family members of employees should seek the standard verification information from each family member. In these circumstances credit unions should follow the guidance in Part I, paragraphs 5.3.72–5.3.116.

Live or work credit unions

- 4.25. In addition to the employee common bond, increasing numbers of credit unions are adopting the common bond ‘live or work’. This means that the qualification for membership of a live or work credit union extends both to residents and to those in regular employment within a particular locality.

¹² Someone in a position of responsibility, who knows, and is known by, the member, and may reasonably confirm the member’s identity. It is not possible to give a definitive list of such persons, but the following may assist in determining who is appropriate in any particular case: the Passport Office has published a list of those who may countersign a passport at www.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174151; and others might include members of a local authority, staff of a higher or further education establishment, or a hostel manager.

FINAL BOARD APPROVED

- 4.26. Live or work credit unions that extend their services to employees of local employers will, however, have similar AML/CTF issues to credit unions linked to just one sponsoring employer so should refer to paragraphs 4.21-4.24 above.

Credit union activity in schools

- 4.27. Many credit unions have established links with their local schools. For many credit unions, establishing partnerships with local schools is a key part of their long-term development strategy. Under a risk-based approach in terms of membership profile and level of activity undertaken by junior savers, credit unions can reasonably assume that children saving in a savings club set up through a school present a lower risk of the credit union being used for money laundering purposes. **Credit Unions must, however, monitor the junior accounts, inter alia to ensure that adults are not laundering through the account.**
- 4.28. Where any potential member cannot reasonably be expected to produce detailed evidence of identity, it should not be a consequence that they are denied access to financial services. If a credit union decides that a particular child cannot reasonably be expected to produce such evidence, the reasons for adopting the 'financial exclusion' approach should be clearly documented. In relation to a schoolchild, a credit union should follow the guidance in Part I, paragraphs 5.3.118 and 5.3.120. In cases where standard identification evidence is not available, it may accept a letter or statement from an appropriate person as evidence of identity. In such cases, a letter from the school should include the date of birth and permanent address of the pupil on the school's letter headed paper to complete standard account opening procedures.
- 4.29. In cases where there is an adult signatory to the account and the adult has not previously been identified to the relevant standards because they do not already have an established relationship with the credit union, the identity of that adult must be verified, in addition to the identity of the child, see Part I, paragraph 5.3.120.

Junior Savers

- 4.30. In addition to offering a credit union service to minors through schools' clubs, many credit unions offer children a savings facility direct with the credit union. In such cases, credit unions should seek identification evidence as set out in Part I, paragraphs 5.3.118–5.3.120. Where standard identification cannot be produced for the child, other evidence such as a letter from the school which includes the date of birth and permanent address of the pupil on the school's letter headed paper, should be sought to complete standard account opening procedures.
- 4.31. Often, the junior account will be established by a family member or guardian. In cases where the adult opening the account has not previously been identified to the relevant standards because they do not already have an established relationship with the credit union, the identity of that adult must be verified, in addition to the identity of the child, see Part I, paragraph 5.3.120.

Enhanced due diligence

- 4.32. There will be certain occasions when enhanced due diligence will be required, for example:
- when the person is involved in a business that is determined to present a high risk of money laundering; examples of high risk businesses can be found in paragraphs 1.36-1.38 of sector 1: *Retail banking*
 - When the proposed customer relationship or transaction is with a person established in a high risk non-EEA country;

FINAL BOARD APPROVED

- where the customer is a PEP, or a family member or close associate of a PEP
- Where a customer has provided false or stolen identification documentation or information on establishing a relationship;

Additional customer information

- 4.33. Credit unions will need to hold sufficient information about the circumstances of members in order to monitor their activity and transactions. Therefore 'Knowing Your Customer' is about building a relationship with the membership and knowing when to ask the appropriate questions at the appropriate time. Reasonable enquiries of a member, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of knowing the customer and monitoring, and should not give rise to tipping off. Although not a prescriptive list, examples of when additional customer information is needed include: a change in circumstances (name, address, employer), a lump sum payment or a change in transaction behaviour. Credit unions may detect significant changes in circumstances when for example, carrying out a loan application, which may require the credit union to seek further information, and to update member profiles which are used as the basis of monitoring customer transactions.
- 4.34. Credit unions must also obtain information about the nature and purpose of the relationship with the member. In the majority of cases, this may be obvious from the service provided, but the credit union may also be providing loans to sole traders for business purposes and information on such relationships must be obtained.
- 4.35. The extent of information sought and of the monitoring carried out in respect of any particular member will depend on the money laundering and terrorist financing risk that they present to the credit union. Credit unions should also have regard to the guidance in Part I, section 5.5.

Monitoring customer activity

- 4.36. As mentioned in paragraphs 4.8-4.9, credit unions must establish a process for monitoring member transactions and activities which will highlight unusual transactions and those which need further investigation. It is important that appropriate account is taken of the frequency, volume and size of transactions. Although not a prescriptive list, an example of a simple approach for credit unions that deal mainly in small sum transactions may be: to investigate deposits over a certain amount, frequency of members' deposits and members whose deposits may appear erratic. However, for larger credit unions that have more complex operational structures, a more sophisticated approach may be needed, e.g., asking who is making deposits in relation to a junior account.
- 4.37. The key elements to monitoring are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and to ask pertinent questions to elicit the reasons for unusual transactions.
- 4.38. Also key to a successful monitoring process is staff and volunteer alertness (see Part I, Chapter 7).
- 4.39. Credit unions must be aware that unusual does not always mean suspicious and therefore should not be the routine basis for making reports to the NCA. Identifying what is unusual is only the starting point – firms need to assess whether what is unusual gives rise to suspicion and report accordingly.

Reporting

FINAL BOARD APPROVED

- 4.40. General guidance on reporting is given in Part I, Chapter 6. All staff and volunteers need to know the identity of the nominated officer, so that they know to whom to report suspicious activity.
- 4.41. It is up to the nominated officer to investigate whether or not to report to the NCA. If he decides not to make a report to the NCA, the reasons for not doing so should be clearly documented and retained with the internal suspicion report. If the nominated officer decides to make a report to the NCA, this must be done promptly and as soon as is practicable. When a report is made to the NCA, the basis for the knowledge or suspicion of money laundering should be set out in a clear and concise manner (see Part I, paragraphs 6.37–6.38) with relevant identifying features for the main or associated subjects. Staff should also familiarise themselves with the consent provisions in POCA and the Terrorism Act (see Part I paragraphs 6.45–6.59) and act accordingly. Furthermore if, under the Data Protection Act a member submits a subject access request, then the credit union should contact the NCA for advice (see Part I, paragraphs 6.90–6.99).

Training

- 4.42. General guidance on staff awareness, training and alertness is given in Part I, Chapter 7. In particular:
- Staff must be made aware of the risks of money laundering and terrorist financing, the relevant legislation and their obligations under that legislation
 - Staff must be made aware of the identity and responsibilities of the firm's nominated officer and MLRO
 - Staff must be trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions
 - Staff training must be given at regular intervals, and details recorded
 - The senior manager or director with ultimate responsibility for AML systems and controls, as required by SYSC 6.3.8 is responsible for ensuring that adequate arrangements for training are in place
 - The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place.
- 4.43. There is no single solution when determining how to deliver training; on-line learning can provide an adequate solution but for some staff and volunteers an on-line approach may not be suitable. Procedure manuals can raise staff and volunteer awareness but their main purpose is for reference. More direct forms of training will usually be more appropriate.
- 4.44. Whatever the approach to training, it is vital to establish comprehensive records to monitor who has been trained, when they received the training, the nature of training given and its effectiveness.
- 4.45. AML/CTF training and training on the responsibility of staff under the firm's own AML/CTF arrangements must be provided to all relevant employees at appropriate intervals.

Internal controls and record-keeping

- 4.46. General guidance on internal controls is given in Part I, Chapter 2, and on record-keeping in Part I, Chapter 8. In particular, credit unions must retain:
- copies of any documents or information obtained to satisfy the CDD measures required under the ML Regulations, until five years after the end of the customer relationship

FINAL BOARD APPROVED

- details of customer transactions for five years after the end of the customer relationship
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report where no external report is made

4.47. Retention of records can be:

- by way of original documents
- photocopies of original documents, taken by credit union staff
- on microfilm
- in scanned form
- in computerised or electronic form

4.48. In relation to internal suspicion reports, the following should be recorded:

- all suspicions reported to the nominated officer
- any written reports by the nominated officer, which should include full details of the customer who is the subject of concern and as full a statement as possible
- all internal enquiries made in relation to the report

5: Wealth management

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

5.1 Wealth management is the provision of investment services including advice, discretionary fund management and brokerage to private investors, ranging from the mass affluent to high and ultra-high net worth individuals (HNWI and UHNWI). Some wealth managers are parts of banks or private banks and may also provide banking services to the same clients. The services are characterised by their bespoke nature tailored to a client's particular needs and may comprise some or all of the following:

- Execution only brokerage (see Sector 10)
- Personalised and detailed advice
- Discretionary portfolio management (see Sector 9)
- Financial planning (see Sector 6)
- Bespoke investment solutions
- Investments in markets in a wide range of jurisdictions, including emerging markets, small investment centres, and metropolitan countries
- high value transactions (for HNWI and UHNWI)
- Current account banking (where the wealth manager is part of a private bank).

What are the money laundering risks in wealth management?

Inherent risks

5.2 Money launderers are attracted by the availability of specialised products and the provision of services that operate internationally, utilise detailed knowledge of clients, create a secure and reputable wealth management environment and are familiar with transactions for private investors. This generates a layer of respectability that 'covers' criminal activity and, it is felt, protects it from investigation. The following factors contribute to the vulnerability of wealth management:

- Wealthy and powerful clients: Such clients may be reluctant or unwilling to provide adequate documents, details and explanations. The situation with regard to them is exacerbated where the client enjoys a high public profile, and may fall into the category of Politically Exposed Person (PEP), indicating that they wield or have recently wielded political or economic power or influence.
- Multiple and complex accounts: wealthy clients often have many accounts in more than one jurisdiction, either within the same firm or group, or with different firms. In the latter situation it may be more difficult for wealth managers to accurately assess the true purpose and business rationale for individual transactions
- Cultures of confidentiality: better off Wealth management clients may seek extra reassurance that their need for confidential business will be conducted discreetly will be met. However, requests for confidentiality should not lead to unwarranted levels of secrecy that suit those with criminal intentions.

FINAL BOARD APPROVED

- Concealment: The use of services such as offshore trusts and the availability of structures such as shell companies in some jurisdictions helps to maintain an element of secrecy about beneficial ownership of funds and may give rise to significant misuse. Care should be taken to ensure that use of banking and investment services in such countries does not facilitate the development of layers of obscurity that assist those with criminal intentions.
- Jurisdictions maintaining statutory banking secrecy: there is a culture of secrecy in some jurisdictions, supported by local legislation, in which wealth management clients may hold accounts without being detected as doing so; it is very difficult if not impossible to investigate whether these accounts have been used for laundered money.
- Corrupt jurisdictions: there are jurisdictions where corruption is known, or perceived, to be a common method of acquiring personal wealth. Attempts may be made to launder assets gained from corrupt practices in these jurisdictions through wealth management firms.
- Movement of funds: The transmission of funds and other assets by private clients may involve high value transactions, and rapid transfers of wealth across accounts in different countries and regions of the world; this can facilitate the concealment of illicit funds before the authorities can catch up with them.
- The use of concentration accounts: i.e. multi-client pooled/omnibus type accounts these are used to collect together funds from a variety of sources for onward transmission and can hide laundered money in the pooling; they are seen as a potential major risk.
- Credit: the extension of credit to clients who use their assets as collateral also poses a money laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.
- Commercial activity conducted through a personal account, or personal activity conducted through a business account, are methods that can be used to deceive the firm or its staff.

Secured loans

- 5.3 Secured loans, where collateral is held in one jurisdiction and the loan is made from another, are common in the private banking areas of wealth management. Such arrangements may serve a legitimate business function and make possible certain transactions which may otherwise be unacceptable due to credit risk. But they may also make it easier to conceal the sources of illicit funds. Collateralised loans raise different legal issues depending on the jurisdiction of the loan, but foremost among these issues are the propriety and implications of guarantees from third parties (whose identity may not always be revealed) and other undisclosed security arrangements that may hide the true nature of the collateral. Particular care should be taken where the lender is relying upon the guarantee of a third party not otherwise in a direct business relationship, and where the collateral is not in the same jurisdiction as the lending firm.

Assessment of the risk

- 5.4 The role of the relationship manager is particularly important to the wealth management firm in managing and controlling and mitigating the money laundering or terrorist financing risks it faces. Wealth management relationship managers develop strong personal relationships with their clients, which facilitates the collection of the necessary information to know the client's business and financial affairs, including knowledge of the source(s) of the client's wealth.

FINAL BOARD APPROVED

However, wealthy clients can have business affairs and lifestyle that may make it difficult to establish what is “normal” and therefore what may constitute unusual behaviour.

- 5.5 Relationship managers must, however, at all times be alert to the risk of becoming too close to the client and to guard against the risks from:
- a false sense of security
 - conflicts of interest which may compromise the firm’s ability to meet its AML obligations and its wider financial crime responsibilities under SYSC
 - undue influence by others , especially by the clients themselves.
- 5.6 As in all firms, relationship managers and other client-facing staff in the wealth management sector should be alert to any developing risk to their personal safety. Criminals seeking to gain advantage from using a firm’s credibility are known to compromise, and sometimes threaten, the firm or its staff. Firms should have:
- suitable internal procedures requiring staff to report when they believe that they have been menaced
 - a policy for reporting incidents to the police

Cash transactions

- 5.7 Relationship managers should neither accept cash nor deliver cash, nor other stores of value such as travellers’ cheques, to anyone. A client should be required to deposit or withdraw cash at the counter of a recognised bank that is at least subject to local supervision. In extremely rare circumstances where this is not possible, there should be a documented policy and procedures in relation to the handling of cash and other stores of value by relationship managers. Such transactions should be reported upwards within the firm’s UK structure and consideration given to informing the firm’s nominated officer.

Customer due diligence

- 5.8 Within the firm, the relationship manager will often be aware of any special sensitivity that may genuinely relate to the client’s legitimate commercial activities or need for personal security.
- 5.9 To control any risk of money laundering, the client’s justification for using financial institutions, businesses or addresses in different jurisdictions should always be subject to scrutiny before undertaking a transaction. To be able to view and manage the risk of money laundering across the whole of the firm or group’s business connections, the wealth manager should consider nominating a senior person to lead such client relationships. The lead relationship manager should have access to sufficient information to enable them to:
- know and understand the business structure
 - determine whether or not there is cause to suspect the presence of money laundering
- 5.10 Ordinarily, the level of diligence carried out in wealth management will be higher than that needed for normal retail banking (see sector 1: *Retail banking*) or investment management (see sector 9: *Discretionary and advisory investment management*) purposes. A wealthy retail client’s needs entailing the use of sophisticated products and fiduciary services, sometimes involving more than one jurisdiction, including trusts, private investment vehicles and other company structures, require careful scrutiny. Where such legal vehicles and structures are used, it is important to establish that their use is genuine and to be able to check the sources of funds and follow any chain of title to know who the beneficial owner is.

FINAL BOARD APPROVED

5.11 In addition to the standard identification requirement in Part I, paragraphs 5.3.57 – 5.3.67, any wealth management service should have particular regard to the following:

- As a minimum requirement to counter the perceived and actual risks, the firm, and those acting in support of the business, must exercise a greater degree of diligence throughout the relationship which will be beyond that needed for normal retail banking purposes. The firm must endeavour to understand the nature of the client's business and consider whether it is consistent and reasonable, including:
 - the origins of the client's wealth
 - Where possible and appropriate, documentary evidence relating to the economic activity that gave rise to the wealth
 - the nature and type of transactions
 - the client's business and legitimate business structures
 - for corporate and trust structures - the chain of title, authority or control leading to the ultimate beneficial owner, settler and beneficiaries, if relevant and known
 - Where appropriate, the reasons a client is using complex structures
 - the use made by the client of products and services
 - the nature and level of business to be expected over the account
- The firm must be satisfied that a client's use of complex business structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

5.12 For some clients, fame is generally recognised as having a long continuing existence, and their photographs are commonly published in the public domain. In such cases, so long as the relationship manager has met the client face-to-face, firms may wish to introduce a controlled procedure, as part of the verification process, whereby the relationship manager may certify a published photograph as having a true likeness of the client. The certified photograph should be retained as a formal record of personal identification.

Recording of visits to the client's premises

5.13 As mentioned in Part I, paragraph 5.3.65, visiting clients can be an important part of the overall customer due diligence process. In wealth management, where possible relationship managers should visit their clients at their place of business in order to substantiate the type and volume of their business activity and income, or at their home if the business factor is not so relevant. The relationship manager who undertakes the visit should make a record by documenting:

- the date and time of the visit
- the address or addresses visited
- a summary of both the discussions and assessments
- any commitments or agreements
- any changes in client profile
- the expectations for product usage, volumes and turnover going forward
- any international dimension to the client's activities and the risk status of the jurisdictions involved

The client profile should be updated where appropriate.

Approval of new relationship

5.14 All new wealth management clients should be subject to independent review, and appropriate management approval and sign off.

FINAL BOARD APPROVED*References*

- 5.15 Reputational searches should be undertaken as a normal part of customer due diligence, which will include checks for negative information. It will sometimes be appropriate to obtain a satisfactory written reference or references from a reputable source or sources before opening an account for a client. The relationship manager should document the nature and length of the relationship between the referee and the client. References should only be accepted when they are:
- received direct – not from the client or third parties
 - specifically addressed only to the firm
 - verified as issued by the referee

Review of client information

- 5.16 The firm's policies and procedures should require that the information held relating to wealth management clients be reviewed and updated on a periodic basis, or when a material change occurs in the risk profile of a client. Periodic review of particular clients will be made on a risk-based basis. Wealth management firms should consider reviewing their business with higher risk clients on at least an annual basis.

Enhanced due diligence (EDD)

- 5.17 Greater diligence should be exercised when considering business with customers who live in high-risk countries, or in unstable regions of the world known for the presence of corrupt practices. Firms must comply with the EDD requirements in the ML Regulations in respect of clients who are PEPs, see Part I, section 5.5 and paragraph 5.20 below.
- 5.18 Those types of client that pose a greater money laundering or terrorist financing risk should be subject to a more stringent approval process. Their acceptance as a client or the significant development of new business with an existing higher risk client should be subject to an appropriate approval process. That process might involve the highest level of business management for the wealth management operation in the jurisdiction. Firms should consider restricting any necessary delegation of that role to a recognised risk control function.
- 5.19 In the case of higher risk relationships, appropriate senior personnel should undertake an independent review of the conduct and development of the relationship, at least annually.

Politically exposed persons (PEPs)

- 5.20 Firms offering a wealth management service should have particular regard to the guidance in relation to PEPs set out in Part I, paragraphs 5.5.13 to 5.5.31. Relationship managers should endeavour to keep up-to-date with any reports in the public domain that may relate to their client, the risk profile or the business relationship.

Other clients

- 5.21 Firms should consider conducting similar searches against the names of their prospects for business, including those that may only be known within the business development or marketing functions; and where practicable, third party beneficiaries to whom clients make payments.
- 5.22 It is recommended that in addition to the categories of client regarded as PEPs, clients connected with such businesses as gambling, armaments or money service businesses should be

FINAL BOARD APPROVED

considered for treatment as high risk. In determining whether to do business with such high risk interests, firms should carefully weigh their knowledge of the countries with which the client is associated as well as the nature of the business that has generated the wealth. Particular consideration should be given to the extent to which their AML/CTF legislation is comparable to the provisions of the relevant EU Directive.

Transaction Monitoring

5.23 General guidance on monitoring customer transactions and activity is given in Part I, section 5.7. In view of the risk associated with wealth management activities, it is appropriate that there should be a heightened ongoing review of account activity and the use made of the firm's other products. In the case of wealth management, the triggers for alerts may be set at a different level, to reflect the appropriate level of control that is to be exercised.

5.24 An illustrative (but not exhaustive) list of matters firms should carefully examine includes:

- substantial initial deposits proposed by prospects for business;
- transactional activity - frequent or substantial activity that is inconsistent with the normal levels associated with the product or purpose - unusual patterns of activity may be evidence of money laundering;
- wire transfers - frequent or substantial transfers not in keeping with either normal usage for the product or the verified expectations of the client's business requirement;
- cash or other transactions - which are not in line with either the normal usage for the product or the verified expectations of the client's business requirement;
- significant increase or change in activity – increased values, volumes or new products required, which do not align with the firm's profile of the client;
- accounts of financial institutions not subject to supervision in an assessed low risk jurisdiction; and
- any activity not commensurate with the nature of the business.

Firms should remain mindful of the possibility of clients using their legitimate resources to finance terrorism.

5.25 Incoming and outgoing transfers, whether of cash, investments or other assets, should be reviewed by the relationship manager or their delegate as soon as is reasonably practicable after the transaction. To ensure the process is efficient, firms will wish to set a threshold figure that is in line with the business risk profile.

5.26 In view of the nature of wealth management services generally, it is appropriate that additional controls and procedures should be applied both to the acceptance and ongoing maintenance of wealth management relationships. These additional controls will also be appropriate when considering the further development of the business relationship with, say, the introduction of new funds or assets, or new technological processes .

6: Financial advisers (including financial planners)

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 6.1 Financial advisers give customers advice on their investment needs (typically for long-term savings and pension provision) and selecting the appropriate products, and on tax issues related to these investments.

Typical customers

- 6.2 The typical customers of financial advisers are personal clients (including high net worth individuals), trusts, companies and charities. .
- 6.3 Financial advisers, whether they only give advice or whether they act on behalf of their customers in dealing with a product provider, are subject to the full provisions of UK law and regulation relating to the prevention of money laundering and terrorist financing. The guidance in Part I therefore applies to financial advisers.
- 6.4 Other sectoral guidance in Part II that is relevant to financial advisers includes:
- Sector 5: *Wealth Management*
 - Sector 7: *Life assurance, and life-related pensions and investment products*
 - Sector 8: *Non-life providers of investment fund products*
 - Sector 9: *Discretionary and advisory investment management*
- 6.5 Generally, financial advisers do not hold permission from the FCA to handle client money, so in practice there is unlikely to be any involvement in the placement stage of money laundering. There is, however, considerable scope for financial advisers being drawn in to the layering and integration stages.
- 6.6 Whether or not financial advisers hold permission to handle client money, they should consider whether their relationship with their customers means that the guidance in sector 5: *Wealth management* or in sector 9: *Discretionary and advisory investment management* applies more directly to them.

What are the money laundering or terrorist financing risks for financial advisers?

- 6.7 The vast majority of financial advice business is conducted on a face-to-face basis, and investors generally have easy access to the funds involved.
- 6.8 Some criminals may seek to use financial advisers as the first step in integrating their criminal property into the financial system.
- 6.9 The offences of money laundering or terrorist financing include aiding and abetting those trying to carry out these primary offences, which include tax evasion. This is the main risk generally faced by financial advisers. In carrying out its assessment of the risk the firm faces of becoming involved in money laundering or terrorist financing, or entering into an arrangement to launder criminal property, the advisory firm must consider the risk related to the product, as well as the risk related to the client.

FINAL BOARD APPROVED

- 6.10 Clearly, the risk of being involved in money laundering or terrorist financing will increase when dealing with certain types of client, such as offshore trusts/companies, politically exposed persons and customers from higher risk or non-FATF countries or jurisdictions, and may also be affected by other service features that a firm offers to its customers. Customer activity, too, such as purchases in secondary markets – for example, traded endowments – can carry a higher money laundering risk.

Customer due diligence

- 6.11 Having sufficient information about customers and beneficial owners, and using that information, underpins all other anti-money laundering procedures. A firm must not enter into a business relationship until the identity of all the relevant parties to the relationship has been verified in accordance with the guidance in Part I, Chapter 5. Depending on the nature of their business, firms should also have regard to the requirements of product providers (see Part II sectors, 7, 8 and 9).
- 6.12 When a full advice service is offered, the process will involve information gathering, an understanding of the customer's needs and priorities and anticipated funds available for investment. The amount of information held about a client will build over time, as there will often be ongoing contact with the customer in order to review their circumstances. However, the level of information held about a customer will be limited if business is transacted on an execution-only or direct offer basis and financial advisers should have an increased regard to the monitoring of business undertaken in this way.

Whose identity should be verified?

- 6.13 Guidance on who the customer is, whose identity has to be verified, is given in Part I, paragraphs 5.3.2 to 5.3.7. Guidance on who the beneficial owner is, whose identity also has to be verified, is given in Part I, paragraphs 5.3.8 – 5.3.13 generally, and in Part II sector 7, Annex 7-I, FAQs, increased risk (v), specifically for investment bonds.

Private individuals

- 6.14 Guidance on verifying the identity of private individuals is given in Part I, paragraphs 5.3.57 to 5.3.105. Guidance on circumstances where it may be possible to use the source of funds as evidence of identity is given in Part I, paragraphs 5.3.82 to 5.3.87.
- 6.15 The firm's risk assessment procedures will take account of the money laundering and terrorist financing risks identified in the sectors in which the relevant product provider operates (see paragraph 6.4). Customers may be assessed as presenting a higher risk of money laundering, whether because he is identified as being a PEP, or because of some other aspect of the nature of the customer, or his business, or its location, or because of the product features available. In such cases, the firm must conduct enhanced due diligence measures (see Part I, section 5.5) and will need to decide whether it should require additional identity information, and/or whether to verify additional aspects of identity. For such customers, the financial adviser will need to consider whether to require additional customer information (see Part I, section 5.5) and/or whether to institute enhanced monitoring (see Part I, section 5.7).
- 6.16 Some persons cannot reasonably be expected to produce the standard evidence of identity. This would include persons such as individuals in care homes, who may not have a passport or driving licence, and whose name does not appear on utility bills. Where customers cannot produce the standard identification evidence, reference should be made to the guidance set out in sector 1: *Retail banking*, Annex 1-I.

FINAL BOARD APPROVED*Non-personal customers*

6.17 Guidance on verifying the identity of non-personal customers is given in Part I, paragraphs 5.3.106 to 5.3.272. Categories of non-personal customers that are likely to be of particular relevance to financial advisers are:

- Private companies (paragraphs 5.3.163 to 5.3.176)
- Partnerships and unincorporated businesses (paragraphs 5.3.177 to 5.3.191)
- 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)

Non face-to-face

6.18 Non face-to-face transactions can present a greater money laundering or terrorist financing risk than those conducted in person because it is inherently more difficult to be sure that the person with whom the firm is dealing is the person that they claim to be. Verification of identity undertaken on a non-face-to-face basis should be carried out in accordance with the guidance given in Part I, paragraphs 5.3.85 to 5.3.89.

Using verification work carried out by another firm

- 6.19 The responsibility to be satisfied that a customer's identity has been verified rests with the firm entering into the transaction with the customer. However, where two or more financial services firms have an obligation to verify the identity of the same customer in respect of the same transaction, in certain circumstances one firm may use the verification carried out by another firm. Guidance on the circumstances in which such an approach is possible, and on the use of pro-forma confirmation documentation, is given in Part I, section 5.6.
- 6.20 Financial advisers should bear in mind that they are often the party which is carrying out the initial customer identification and verification process. As such, it is they who will be asked to confirm to a product or service provider that such verification has been carried out. Although not directly related to the sort of work that financial advisers typically carry out, the significance of issuing such confirmations is highlighted by the actions of the then FSA in 2005 in fining a bond broker who gave such confirmation when he was aware that he had not, in fact, carried out appropriate customer due diligence.
- 6.21 Product providers often rely on customer verification procedures carried out by financial advisers, which underlines the importance of their systems and procedures for risk assessment being effective.
- 6.22 Where the financial adviser has carried out verification of identity on behalf of a product provider, the adviser must be able to make available to the product provider, on request, copies of the identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained by the adviser (see paragraph 6.29). This obligation extends throughout the period for which the financial adviser has an obligation under the ML Regulations to retain these data, documents or other information.

Suspicious transactions

6.23 Financial advisers are ideally placed to identify activity which is abnormal, or which does not make economic sense, in relation to a person's circumstances. Obtaining details on the source of a customer's wealth, and identifying the purpose of an activity are all mandatory parts of the

FINAL BOARD APPROVED

normal advice process. Financial advisers do not have to handle the transaction personally to have an obligation to report it.

- 6.24 Guidance on monitoring customer transactions and activity is set out in Part I, section 5.7. Guidance on internal reporting, reviewing internal reports and making appropriate external reports to the NCA, is given in Part I, Chapter 6. This includes guidance on when a firm needs to seek consent to proceed with a suspicious transaction, with which financial advisers need to be familiar.

Staff awareness and training

- 6.25 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions, which may prove to be suspicious.
- 6.26 Guidance on staff awareness, training and alertness is given in Part I, Chapter 7. This guidance includes suggested questions that staff should be asking themselves, and circumstances that should cause them to ask further questions about particular transactions or customer activity.

Record-keeping

- 6.27 General guidance on record-keeping is given in Part I, Chapter 8. The position of financial advisers means that some of the guidance in Part I, Chapter 8 cannot easily be applied. Generally, financial advisers will verify customers' identities by means of documentation, as they will often not have access to electronic sources of data. Where documents are used, it is preferable to make and retain copies.
- 6.28 Financial advisers may, from time to time, be asked by product providers for copies of the identification evidence that they took in relation to a particular customer. Financial advisers' record-keeping arrangements must therefore be capable of enabling such material to be provided in a timely manner (see Part I, paragraph 5.6.18).
- 6.29 Documents relating to customer identity must be retained for five years from the date the business relationship with the customer has ended (see Part I, paragraph 8.12).

7: Life assurance and life-related protection, pension and investment products

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance and the frequently asked questions in appendix ??.

- 7.1 This sectoral guidance helps firms to interpret how the risk-based approach set out in Part I, Chapter 4 and the customer due diligence requirements set out in Part I, Chapter 5 might be applied to the specific circumstances of the protection, savings and pensions businesses of the insurance sector.

What are the money laundering risks in the protection, pension and investment business of the insurance sector?

- 7.2 The insurance sector provides a diverse range of products to customers via an equally diverse range of distribution channels. It has been noted that the majority of insurance products do not deliver sufficient functionality and flexibility to be the first choice of vehicle for the money launderer. However, given changes brought about by pensions freedoms and an ever more diverse range of products being offered, this risk will continually evolve and firms need to take this into account when conducting their risk assessments. It is also recognised that although the nature of certain products helps reduce the money laundering risk, the funds used to purchase them could still be the proceeds of crime. Where there are doubts as to the legitimacy of the transaction, verification of the customer's identity remains important as part of the investigation into the transaction and the customer.

The key drivers of risk

- 7.3 Part I, Chapter 4 states that any risk-based approach to AML needs to start with the identification and assessment of the risk that has to be managed and identifies key elements (or drivers) of risk as follows:
- products and services offered (including product features)
 - party (e.g. the customer and any associated party such as the beneficial owner);
 - jurisdictions operating in /overseas connections;
 - distribution channels (to deliver the products, services and transactions); and
 - the complexity and volume of transactions and payment methods.
- 7.4 In addition to the risks identified above, the increasing volume of activities outsourced by insurers brings an additional dimension to the risks that the insurer faces, and this risk must be actively managed - see Part I (2.7 ff). Insurers that outsource activities should assess any possible AML/CTF risk associated with the outsourced functions, record the assessment and monitor the risk on an ongoing basis.
- 7.5 FCA regulated firms cannot contract out of their regulatory responsibilities, and they remain responsible for systems and controls in respect of the activities outsourced, whether within the UK or to another jurisdiction. In all instances of outsourcing, it is the delegating firm that bears the ultimate responsibility for the duties undertaken in its name. This includes ensuring, via relevant periodic reviews that the provider of the outsourced activities has satisfactory AML/CTF systems, controls and procedures.

FINAL BOARD APPROVED

- 7.6 Based on the views of insurance firms, the majority of this guidance focuses on risks from a product-led perspective; however, there are circumstances in which a customer's profile, activity and complexity of transaction may add to the product risk. This is particularly the case with regard to Politically Exposed Persons – see Part I (5.5.13 ff). A firm must ensure that their own risk-based approach is appropriate to the particular circumstances they face – see Part I (4.24ff)

Politically Exposed Persons (PEP)

- 7.7 Part I (5.5.13 ff) sets out general provisions for identifying, establishing business with, and monitoring PEPs. This sectoral guidance sets out the fundamental risks and business practices that insurers may wish to consider when developing a risk-based procedure. These risks and business practices may change, and it is therefore important that insurers monitor these developments and adjust their procedures accordingly.
- 7.8 When developing a procedure for identifying PEPs, insurers should target those areas of business that are at the greatest risk of having customers who meet the PEP criteria.
- 7.9 Firms may consider using criteria such as accounts with non-UK residents¹³ and investment value to determine their risk-based approach to PEP identification and additional information can be found in the FCA PEP guidance.
- 7.10 It is expected that this risk-based procedure will make the volume checking of new customers unnecessary. However, adequate measures to check PEP status for those customers meeting the high risk criteria should be undertaken during the course of establishing the business relationship. If a PEP is identified at this stage, senior management approval is required for establishing a business relationship. In the case of identifying an existing customer as a PEP, senior management approval for continuing the business relationship must be obtained as soon as practicable upon identifying a PEP.
- 7.11 The identification of a customer as a PEP is not in itself cause for suspicion, and must not be used for reason to reject or exit a business relationship, but requires an enhanced level of due diligence in line with the guidance set out in Part I. FCA-regulated firms should also have regard to the separate guidance on the treatment of PEPs published by the FCA in July 2017. In some cases enhanced due diligence may trigger suspicions that the client is attempting to store or launder the proceeds of crime, including corruption. In such cases, a SAR and consent request must be submitted to NCA, following the guidance set out in Part I, chapter 6.

Geographical Risk

- 7.12 Jurisdiction risk must be taken into account when a party is located overseas, a payment has been received from overseas or a payment has been requested to be made overseas. Part I, chapter 5 provides further guidance. Insurers may have exposure to jurisdiction risk when existing customers move overseas, overseas customers are sold UK products or associated parties such as beneficial owners are located overseas. When this is the case, due regard must be paid to the firm's assessment of jurisdiction risk. Further information can be found in Part I, chapter 5.

Distribution Risk

- 7.13 The distribution channel for products may alter the risk profile. For insurers the main issues

¹³ For the purposes of this guidance, a non UK resident is a person defined as such for UK tax purposes.

FINAL BOARD APPROVED

will be non face-to-face sales, such as online, postal or telephone sales.

- 7.14 For business sold through agencies, such as financial advisers, agency acceptance and ongoing management procedures may already meet the requirements set out in Part I, paragraphs 5.6.26 and 5.6.27. The MLRO should ensure that he is comfortable with the vetting processes undertaken by the firms distribution arm, for advisers, prior to the issue of and throughout the agency agreement. This should include the ability of the intermediary to provide copies of the underlying documents or data on request. The MLRO should be aware and satisfied with the level of monitoring of any material breaches/financial difficulties, which might call into question the agent's status as fit and proper.
- 7.15 Once a business relationship is established with an intermediary, the Confirmation of Verification of Identity is the record for the purpose of meeting the record keeping requirements (this is irrespective of any outsourced administrative arrangement) and should be retained in accordance with the guidance provided in Part I, paragraphs 5.6.4ff. If, in the course of normal business, the intermediary's standards are called into question, the insurer should review its status as a provider of CVIs. For higher risk business, such as non-UK, the MLRO will need to be satisfied that the level of customer due diligence carried out by the third party is commensurate with the risk and may wish to request copies of the underlying evidence obtained by the intermediary.

Product Risk

- 7.16 The remainder of this sectoral guidance concentrates on product risk. This is because, in the insurance sector, the nature of the product being sold is usually the primary driver of the risk assessment. This is because of the different nature of each category of products (protection, pensions and investments) and the fact that each product's features are defined and potentially restricted; i.e., some will only pay out on a verifiable event such as death or illness, whilst others are accessible only after many years of contributions. As well as limiting the flexibility of these products as potential money laundering vehicles, the restrictions also enable firms to more readily profile the products for 'standard' (and conversely, 'non standard' or 'suspicious') use by customers.
- 7.17 A number of products sold by firms in the insurance sector, including General Investment Accounts (GIAs), single premium investment bonds and certain pensions, do feature increased flexibility/risk. This should be acknowledged in the application of the risk-based approach.
- 7.18 The following are features which may tend to increase the risk profile of a product:
- accept payments or receipts from third parties;
 - accept very high value or unlimited value payments or large volumes of lower value payments;
 - accept cash payments;
 - accept frequent payments (outside of a normal regular premium policy);
 - provide significant flexibility as to how investments are managed to be liquidated quickly (via surrender or partial withdrawal) and without prohibitive financial loss;
 - be traded on a secondary market;
 - be used as collateral for a loan and/or written in a discretionary or other increased risk trust;
 - accept overpayments;
 - provide access to funds;
 - available on a Platform.
- 7.19 The following are features that may tend to reduce the risk profile of a product:

FINAL BOARD APPROVED

- restricted capacity to accept third party receipts or make third party payments;
 - have total investment curtailed at a low value due to either the law or a firm's policy;
 - be relatively small value regular premium policies that can only be paid via direct debit;
 - require the launderer to establish more than one relationship with a firm or another official body (e.g., certain types of pension products where the customer has to set up the product with the provider and to get HMRC approval and possibly appoint a Pensioner Trustee);
 - have no investment value and only pay out against a certain event (death, illness etc) that can be checked by the product provider; and/or be linked to known legitimate employment.
- 7.20 The above are general lists of characteristics and are indicative only. Firms are strongly discouraged from using the lists in isolation for a mechanical 'tick box' style exercise. No characteristic acts of itself as a trigger. Not all products that may be used, say, as collateral for a loan, are automatically 'increased risk' by virtue of one characteristic alone. These general characteristics are given so that firms may weigh them up in overall balance for specific, branded products against their knowledge of the customer and their business.
- 7.21 Platform or 'wrapper' product offerings are those where a variety of products are offered to various target markets under an overarching 'wrapper' arrangement. These products may form, in effect, a portfolio arrangement for underlying clients or members, sold via arrangements conducted between the product provider and a third party - typically a regulated introducer (financial adviser), Employer or similar. They may encompass a variety of risk factors that drive the level of customer due diligence (see paragraphs 7.2 to 7.28).
- 7.22 Firms may wish to consider whether they should apply a standard level of customer due diligence to the whole 'platform' or 'wrapper', or whether to graduate the level of customer due diligence dependent on the actual product occurrence and specific risk factors as/when they arise. The customer due diligence should be conducted as appropriate, and before trading commences on the 'platform' or 'wrapper', in accordance with paragraphs 7.1 to 7.57 and financial sanctions guidance in Part III, Section 4. Whichever approach is used, a firm should ensure that it documents its approach and is satisfied that the approach adequately addresses the money laundering and terrorist financing risks according to the combination of risk factors inherent in the 'platform' or 'wrapper' arrangement.
- 7.23 Where apparent inconsistencies exist, firms are expected to exercise judgement accordingly. For example certain pension products and platform based portfolio arrangements accept contributions from employers. Third party payments are normally indicative of increased risk according to the list in 7.18, however for such products, there is some risk reduction in respect of source of funds. Some of the other features of pension products (the restricted access to funds up to the age of 55, and the involvement of HMRC), also reduce the product risk.
- 7.24 It is stressed that risk levels attributed to generic products in this document are intended to provide a starting point for a firm's risk assessment. Firms should consider whether their own, branded versions of those generic products possess features (such as a facility for top up payments or prohibition from receiving /making third party payments) which raise or lower the risk level. Equally, taking account of other risk drivers which might be identified (for example, the geographical location of a customer) may lead a firm to 'upgrade' or downgrade the overall risk level of a product from that indicated in this guidance. Part I, section 5.5 discusses risk drivers that are not specific to insurance products. Also, where a proposition for business involving an intermediate or reduced risk product is exceptional due to the size, source of funds or for another reason that suggests risk of fraud, money laundering or other usage of proceeds of crime additional due diligence will be appropriate perhaps via existing anti-fraud or other business risk management procedures.

FINAL BOARD APPROVED*Three overall risk levels*

- 7.25 Firms in the insurance sector have carried out risk profiling of their products, applying the risk assessment criteria detailed above. This guidance draws on that work and establishes three overall levels of risk for insurance products in an AML context. The risk level determines what work a firm needs to carry out to meet industry standards. The three levels are:
- a) reduced risk;
 - b) intermediate risk; or
 - c) increased risk.
- 7.26 When attributing an appropriate risk level, it is important to keep insurance risk in its wider context. As already noted, the majority of insurance products do not deliver sufficient functionality and flexibility to be the first choice of vehicle for the money launderer.
- 7.27 The products identified as ‘increased risk’ are therefore categorised as such only in the context of the insurance sector and are not intended to equate to references to ‘high risk’ in the wider context of the financial services industry as a whole.
- 7.28 The risk level attributed should always be based on the underlying product, irrespective of how it is described in the product provider’s literature (i.e., substance prevails over form). Firms should expect to be in a position to justify the basis on which the risk assessment criteria have been applied.
- 7.29 Risk management is a continuous process (as noted in Part I, paragraph 4.64). The risk assessment process is not a one-time exercise, and it must be revisited and reviewed on a regular basis.
- 7.30 Finally, there is a need to monitor the environment in which the firm operates. It should be recognised that success in preventing money laundering in one area will tend to drive criminals to migrate to another area, business, or product stream. Firms should be aware of current risk assessments of money laundering/terrorist financing risk in the insurance sector and take them into consideration, along with trends they experience themselves. If displacement is happening, or if customer behaviour is changing, the firm should be considering what it should be doing differently to take account of these changes. A firm's anti-fraud measures will also help it understand its customers and mitigate the money laundering risks.

I - Reduced risk level

- 7.31 Some groups of products, due to their inherent features, are extremely unlikely to be used for money laundering purposes. Some of these are recognised by the Money Laundering Regulations as potentially qualifying for Simplified Due Diligence [See Regulation 37(3)(b)]. Others, such as lifetime annuities are considered part of the pensions product. The table below shows these products in their respective categories of protection and pensions. The table also shows a number of the typical features (or restrictions) of each product, which serve to limit their potential as money laundering vehicles and so qualify them for this risk level.
- 7.32 Risk levels attributed to generic products in this section are intended for guidance only. Firms should consider whether their own branded versions of these generic products have features that either reduce or increase this indicative risk level.

Protection	Rationale	
1 Term life assurance	<i>Typical features:</i>	<i>Timing of verification for pure</i>

	<ul style="list-style-type: none"> ○ Only pays out on death of assured ○ No surrender value ○ Small, regular premiums: additional payments by customer not possible ○ Large premiums will normally require medical evidence ○ No investment element ○ Once term of policy is finished no payout and policy ceases 	protection products (Part I: 5.2.3,) ML Regs 37(3). Part II 7.31
2 Income protection products related to long-term illness	<ul style="list-style-type: none"> ○ Only pays out on medical evidence and proof required as to loss of income ○ No surrender value ○ Small, regular premiums: additional payments by customer not possible 	Timing of verification for pure protection products (Part I: 5.2.3,) ML Regs 37(3), Part II 7.31
3 Critical illness products relating to diagnosis of a specific critical illness	<ul style="list-style-type: none"> ○ Only pays out on medical evidence ○ No surrender value ○ Small, regular premiums: additional payments by customer not possible 	Timing of verification for pure protection products (Part I: 5.2.3), ML Regs 37(3), Part II 7.31
4. Group Life Protection	<ul style="list-style-type: none"> ○ Only pays on medical evidence ○ No surrender value ○ Premiums paid by employer – no member funding ○ Relatively small regular premiums 	Timing of verification for pure protection products (Part I: 5.2.3) ML Regs 37 (3). Part II 7.31
Pensions		
5 Pension, superannuation or similar schemes which provide retirement benefits to employees (see footnote 8), 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 (see	<ul style="list-style-type: none"> ○ Long term savings vehicle - No surrender value ○ Product may not be used as collateral 	Qualifies for Simplified Due Diligence (Part I 5.4.5), ML Regs 37(3)

FINAL BOARD APPROVED

footnote 9)		
6 Pensions annuities, whether purchased with the company running the long-term savings vehicle or through an open market option.	○ <i>Product already subject to due diligence and ongoing monitoring from the pension provider</i>	<i>Qualifies for Simplified Due Diligence. ML Regs 37(3)</i>
7 Rebate Only Personal Pension (“RPP”)	○ <i>Only funded by National Insurance Contribution rebates payable as a result of an individual being contracted out of SERPS or S2P</i>	<i>Qualifies for Simplified Due Diligence</i>
8 Immediate Vesting Personal Pension (“IVPP”). Purchased with the transfer from another pension for the purpose of exercising an open market annuity option.	○ <i>Product already subject to due diligence and ongoing monitoring from the pension provider</i>	<i>Qualifies for Simplified Due Diligence. ML Regs 37(3)</i>

⁸ This would cover Contracted in and out Group Money Purchase Schemes, Final Salary Schemes, Buy Out Plans from the latter types of schemes (if no further contributions are allowed) and Rebate-only schemes.

⁹ This qualification for Simplified Due Diligence is based on the Money Laundering Regulations 2017 37(3)(b).

Customer due diligence

7.33 The recommended industry standard for protection products in this category is for due diligence on the customer and the beneficiary to be carried out at the point of claim. For most circumstances, the counter fraud checks at point of claim will satisfy these requirements.

7.34 For pensions annuities, it is sufficient for the insurer to satisfy itself that the pension scheme funding the annuity is HMRC-registered.

7.35 The recommended industry standard for reduced risk pension products is as follows:

Apply Simplified due diligence. Therefore *apart from monitoring*, standard customer due diligence does not apply to either the customer or the scheme.

However, where a firm considers that there are features of the nature of the employer or the scheme that present an increased risk of money laundering, the following enhanced due diligence measures may be appropriate:

- a. Obtaining details of the trustees and the entity (usually the employer), copy of the relevant trust deeds, and verifying the scheme’s HMRC/PSO number (this can be done, for example, by sight of the scheme’s HMRC approval letter).

Note - HMRC does not now issue approval letters. However, if the firm has any concerns, on application and with the relevant authority, HMRC will provide

FINAL BOARD APPROVED

documentary confirmation regarding the existence of the scheme.

- b. Verifying the identity of the employer, or other corporate entity paying into the fund, in accordance with Part I, Chapter 5. Check that the firm is trading and appropriate to provide employees with a pension through a Companies House search, Persons with Significant Control register (PSC) check or a visit to premises. Beneficial owners should be identified e.g. on the Companies House search or checking the PSC register, however it is not necessary to verify their identities, . Ongoing monitoring, however, is still required.
- 7.36 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a Bankers Draft or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.
- 7.37 In addition, the destination of funds at the time of redemption can be used as evidence of identity in cases where there has not previously been a requirement to verify, for example where the firm had been able to rely on an exemption.
- 7.38 In these cases, depending on the firm's assessment of the risk presented by the situation, including the circumstances in which the customer acquired the investment, it may be possible to satisfy the standard identification requirement by means of a payment to an account with a UK or EU regulated credit institution in the sole or joint name of the customer. The old style Financial Adviser Certificates (confirmations of identity) had a tick box "Existing Customer Pre April 1994" – this exemption is not transferable to Insurers. The firm may, however, have completed a current customer review exercise to pick the verification of these customers up.

Monitoring

- 7.39 Companies must take a risk-based approach to monitoring reduced risk products. Even where simplified due diligence is applied, transaction/activity monitoring should still be undertaken. A company's normal anti-fraud controls should provide a suitably robust system of monitoring. Enhanced monitoring may be considered for those pension holders over the age of 55 years of age to reflect the increased pensions freedoms brought in by the government in 2014. This is reflective of the increased access for these individuals to drawdown and payback into pension pots.

*Frequently asked questions in relation to reduced risk – please see Annex 7-I***II - Intermediate risk level**

- 7.41 The intermediate risk level has been attributed to a group of products whose inherent features pose some risk of use for the purposes of money laundering or terrorist financing but they are significantly less than the risks posed by the "increased risk" grouping of insurance products. Some risk is acknowledged in the case, for example, of products with a facility for 'top up' payments, and therefore the standard level of due diligence is appropriate. The table below shows these products in their respective categories of protection, savings and pensions, together with some of their typical features or restrictions.
- 7.42 Risk levels attributed to generic products in this section are intended for guidance only. Firms should consider whether their own branded versions of these generic products have features that either reduce or increase this indicative risk level.

Protection	
1 Whole of Life	<i>Typical features:</i> <ul style="list-style-type: none"> ○ may accrue some surrender value ○ benefits usually payable on death or diagnosis of terminal illness ○ or, in some cases, critical illness of the policyholder ○ partial surrenders are normally allowed within specified limits ○ qualifying whole of life plans will comply with the rules applicable to qualifying life policies
Savings and Investments	
2 Life assurance savings plan	<i>Typical features:</i> <ul style="list-style-type: none"> ○ Long term savings plan often for retirement ○ Requires at least 5 years to gain positive return on investment ○ Often unable to be surrendered in first or second year, with penalties in years three to five ○ Additional 'top up' payments may be permitted ○ Sum assured/premium relationship broadly complying with HMRC Qualifying Rules
3 Endowments	<ul style="list-style-type: none"> ○ Long term savings plan for a set term, were often linked to mortgages ○ Sum assured/premium relationship broadly complying with HMRC Qualifying Rules ○ Usually long term, 10-25 years
4 Trustee Investment Plan ("TIP")	<ul style="list-style-type: none"> ○ The plans are governed by trustees ○ The plans must be associated with a pension scheme ○ All cash flows into and out of the Plan must be via the trustees ○ Not FCA-regulated
Pensions	
5 Group Personal Pension ("GPP")	<i>Typical features:</i> <ul style="list-style-type: none"> ○ Long term policy, usually up to 40 years ○ No access to funds in normal circumstances until the policyholder reaches 55 years of age ○ Employee and employer contributions
6 Group Stakeholder Plan	<ul style="list-style-type: none"> ○ Long term policy, usually up to 40 years ○ Portable pension pot ○ HMRC registered scheme ○ Annual and lifetime limits apply ○ No access to funds in normal circumstances until the policyholder reaches 55 years of age
7 Income Drawdown Flexible Pension Plan Phased Retirement Plan	<ul style="list-style-type: none"> ○ <i>Typical features:</i> ○ Policies only open to individuals between the ages 55 – 75, and people who have already accrued by a pension fund

FINAL BOARD APPROVED

8 Free Standing Additional Voluntary Contribution Plan (“FSAVC”)	<ul style="list-style-type: none"> ○ Contributions cap set by pensions legislation and monitored by scheme administrator ○ Transfers are only possible to another regulated entity
9 Stakeholder Plan	<ul style="list-style-type: none"> ○ Long term policy, usually up to 40 years ○ No access to funds in normal circumstances until the policyholder reaches 55 years of age ○ HMRC registered scheme ○ Annual and lifetime limits apply
10 Personal Pension Plan (not SIPP or SSAS)	<ul style="list-style-type: none"> ○ Long term policy, usually up to 40 years ○ No access to funds in normal circumstances until the policyholder reaches 55 years of age ○ HMRC registered scheme. Transfers are possible, but only to another registered scheme. ○ Annual and lifetime limits apply.
11 Self Invested Personal Pension (“SIPP”)	<ul style="list-style-type: none"> ○ Provides a choice of allowable investments, including commercial property, i.e., can be used to buy business premises. ○ Long term policy, usually up to 40 years ○ No access to funds in normal circumstances until the policyholder reaches 55 years of age ○ HMRC registered scheme. Transfers are possible, but only to another registered scheme. ○ Annual and lifetime limits apply.
12 Executive Pension Plans (“EPPs”) (excludes CIMPs & COMPs – see Minimal Risk section)	<p><i>Typical features:</i></p> <ul style="list-style-type: none"> ○ Contributions from company to tax exempt fund, normally ○ Established by company directors for their benefit ○ Single premium payments permitted ○ Long term policy, usually up to 40 years ○ No surrender value. ○ HMRC registered scheme. Transfers are possible, but only to another registered scheme. ○ Annual and lifetime limits apply. ○ Not FCA-regulated
13 Small Self Administered Schemes (“SSASs”)	<ul style="list-style-type: none"> ○ Small limited companies where directors are the main shareholders ○ Flexibility of investment options ○ Able to be used to raise loan capital ○ Long term policy, usually up to 40 years ○ No surrender value. ○ HMRC registered scheme. Transfers are possible, but only to another registered scheme. ○ Annual and lifetime limits apply. ○ Not FCA-regulated
14 Immediate Vesting Personal Pension (“IVPP”). Purchased for purposes other than pursuing an open market annuity option.	<ul style="list-style-type: none"> ○ Policies only open to individuals between the ages of 55 and 75. ○ Normally the end product of a pension transfer ○ Annuity usually purchased with one one-off payment to provide income for life.

FINAL BOARD APPROVED

15 Purchased Life Annuity (“PLA”) Hancock Annuity	<ul style="list-style-type: none"> ○ <i>No return of cash lump sum at end of the term selected or when customer dies</i> ○ <i>Once annuity purchased, purchaser cannot alter the arrangements or cash it in.</i>
--	--

- 7.43 As can be seen, the majority of intermediate risk level products are found in the pensions category, which reflects the restricted access to funds in a pension arrangement; pensions cannot be encashed and payments out are limited to tax free cash lump sums (for example, up to 25% of the fund for stakeholder and personal pensions) and regular income. In addition, some schemes will have an independent pensioner trustee who polices the running of the scheme on behalf of HMRC.

Customer due diligence

- 7.44 The recommended industry standard for intermediate risk products is as follows: Verify the identity of the customer and/or the relevant parties, as per the guidance set out in Part I, Chapter 5, at the outset of the business relationship.
- 7.45 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a Bankers Draft or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.
- 7.46 In accordance with Part I, companies must identify the beneficial owner, following the guidance in Part I, paragraphs 5.3.8 to 5.3.13.
- 7.47 In addition, the destination of funds at the time of redemption can be used as evidence of identity in cases where there has not previously been a requirement to verify, for example where the firm had been able to rely on an exemption. In these cases, depending on the firm's assessment of the risk presented by the situation, including the circumstances in which the customer acquired the investment, it may be possible to satisfy the standard identification requirement by means of a payment to an account with a UK or EU regulated credit institution in the sole or joint name of the customer. The old style Financial Adviser Certificates (confirmations of identity) had a tick box “Existing Customer Pre April 1994” – this exemption is not transferable to Insurers. The firm may however have completed a current customer review exercise to pick the verification of these customers up.

Monitoring

- 7.48 Insurance companies should have a programme of monitoring which reflects the intermediate risk status of the products mentioned above. A firm should ensure its employees are adequately trained to identify and report unusual business activity to the firm's nominated officer. Enhanced monitoring may be considered for those pension holders over the age of 55 years of age to reflect the increased pensions freedoms brought in by the government in 2014. This is reflective of the increased access for these individuals to drawdown and payback into pension pots.
- 7.49 Firms should undertake ongoing monitoring for patterns of unusual or suspicious activity to ensure that higher-risk activity can be scrutinised. For example, top-up payments when these are much larger than current holdings, or for EPPs & SSASs, are areas that should receive scrutiny, as well as loans taken out using product as collateral.

Frequently asked questions in relation to intermediate risk – please see Annex 7-I

FINAL BOARD APPROVED

III Increased risk level

- 7.51 The increased risk level has been attributed to a product whose inherent features open the possibility to their being used for money laundering purposes. The product may have a facility for third party and/or 'top up' payments, or is perhaps negotiable, and therefore an enhanced level of due diligence by asking for more information is appropriate. It is to this risk level that the majority of a firm's AML resource will normally be directed. The table below shows the product together with the features.
- 7.52 Risk levels attributed to the generic product in this section are intended for guidance only. Firms should consider whether their own branded versions of this generic product have features that either reduce or increase this indicative risk level. As stated before, the increased designation is used here to reflect the different average levels of investments in pensions, savings and other investment products experienced by firms and intermediaries across the sector.

Protection	
None	
Savings and investments	Typical features:
1 Single premium investment bonds, including: <ul style="list-style-type: none"> • With profits • Guaranteed • Income • Investment • Offshore international bonds 	<ul style="list-style-type: none"> ○ <i>Open ended investment</i> ○ <i>Usually a 5 year recommended minimum investment term but can be surrendered earlier</i> ○ <i>Additional 'top up' payments permitted by policy holder and by third parties</i> ○ <i>May be segmented and individual segments may be assignable</i>
Pensions	
None	

- 7.53 As can be seen from the table above, the increased risk level product is in the investments category, which reflects the higher value premiums that can be paid into them, the relative ease of access to accumulated funds and the lack of involvement of external agencies such as the HMRC.

Customer due diligence

- 7.54 The recommended industry standard for increased risk products is as follows:

1. Verify the identity of the customer, and/or the relevant parties, as per the standard procedures set out in Part I, Chapter 5, at the outset of the business relationship

AND

2. Acquire prescribed information at the outset of the business relationship to satisfy the additional information requirements of Part I, Chapter 5:
 - a. source of funds for the transaction (e.g., a UK bank account in own name);
 - b. employment and salary details; and
 - c. source of wealth (e.g., inheritance, divorce settlement, property sale)

FINAL BOARD APPROVED

3. If the firm determines that the risk of the business is increased further by the customer and/or payment and/or location (e.g. the customer is a PEP in a high risk country), the firm should consider, as part of its EDD, whether the information regarding source of wealth should be evidenced. For example, for source of wealth from inheritance, a copy of the Will could be requested.
- 7.55 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.
- 7.56 An insurer must, where appropriate, verify the identity of the beneficial owner for increased risk products in line with the provisions in Part I, paragraphs 5.3.8 to 5.3.13.

Monitoring

- 7.57 Firms should undertake ongoing monitoring for patterns of unusual or suspicious activity to ensure that higher risk activity can be scrutinised. A firm should ensure its employees are adequately trained to identify and report unusual business activity to the firm's nominated officer.

Frequently asked questions in relation to increased risk – please see Annex 7-I

**Life assurance and life-related protection, pension and investment products –
Frequently asked question**

Reduced risk

- (i) *What if we identify that a third party is / has been paying into a reduced risk protection product?*

Firms should, in the course of their normal commercial business, be considering whether any suspicious or unusual circumstances apply, and should act accordingly, and this might involve verifying the identity of the third party. However, in the absence of such concerns, unless the third party is the beneficiary (who may be verified by counter-fraud checks at point of claim), there is no requirement to verify the identity of the third party premium payer for reduced risk protection products at any stage.

- (ii) *What if there is a change of beneficiary or if payout is made to a third party on one of these reduced risk products?*

Unless the amount of money to be paid out is small and financial crime is not suspected, the identity of the third party must be verified before payout can take place. A letter of instruction from the original beneficiary will not normally suffice.

- (iii) *What if payments into exempt occupational pension schemes begin to be received from the employee rather than from the employer?*

Firms should have adequate procedures and controls to identify where payments are not received directly from the employer but instead are received directly from the employee or another third party, whether by personal cheque or direct debit. Where such payments are received, and where the sums are considered material, standard identification and verification requirements set out in Part I, section 5.4 should be applied to the payer as soon as is reasonably practicable.

- (iv) *How does using the “source of funds” as evidence affect these reduced risk level products?*

- a) For reduced risk level products, firms may accept personal cheques and other payment instruments drawn on a customer’s account as satisfying the requirement to verify the customer’s identity.
- b) Where the funds are being paid into a reduced risk level product by direct debit from an account in the customer’s name, there is no additional requirement on firms to correlate the name on the direct debit instruction with the account details at the outset of the relationship. It is usual practice for firms to undertake further due diligence on the customer’s identity before any payment is made, as part of their fraud prevention procedures. If a firm’s procedures do not provide for further customer due diligence to be undertaken before any payment is made, it should confirm at the outset of the relationship that the payments made by direct debit are made from an account in the name of the client, in accordance with Part I, paragraph 5.3.82.

- (v) *What about verification on reduced risk level pension transfers?*

FINAL BOARD APPROVED

There is no requirement to verify identity if **both** of the following conditions are satisfied:

1. the transfer is **from** an Occupational Pension Scheme which is not a Executive Pension Plan (“EPP”) or a Small Self Administered Scheme (“SSAS”); **and**
2. the transfer is **to** an Occupational Pension Scheme (which is not an EPP or a SSAS) **or** is **to** a S32 buy out plan with no additional funding.

- (vi) *What if a pension-sharing order or pension-earmarking order (for example in the case of a divorce) is received for a reduced risk pension?*

Firms may accept court documents as verification of identity of the existing customer, if this has not already been completed.

Subject(s) of such an order that are explicitly nominated to receive funds should be regarded as the beneficial owner(s), and their identity may also be verified by reference to the court document(s).

- (vii) *What if a payment on death is to be made direct to a beneficiary?*

On short to medium term insurance, payments to beneficiaries on the instructions of the executor or administrator may be made once the beneficiaries have been PEP and sanction screened. If there are no PEP or sanctioned parties involved, there is no need to verify the identity of beneficiary, if the payment is made to an account in their name. However, if a beneficiary wishes to transact any business their own name, or the business is long term insurance their identity will need to be verified in addition to the PEP and Sanction check, in line with the guidance in Part I, section 5.3, and paragraph 5.3.2. Any matches to PEPs and sanctions should be dealt with in line with Part I section 5.5.

- (viii) *What if a payment on death is to be made direct to a trustee of a protection product?*

Where payments, from reduced risk products, are made to the trustees via a Trust Bank account there is normally no need to individually verify the Trustees themselves, as the Trust Bank Account will ensure that the funds remain part of the trust at point of payment. The trustees should be PEP and Sanction checked unless already done so.

However, if a firm decides to make payment other than to a Trust Bank Account (and the firm should ensure that it would not be acting in breach of the Trust by so doing) then it is necessary to individually verify the intended recipient (and conduct sanctions and PEP checks) prior to payment being made.

- (ix) *Is the pensions and annuities risk increased with Pension Liberation and the UK Government’s April 2014 budgetary changes, which remove the requirement to take an annuity and give easier access to pension funds?*

The placement of all products listed in this section into risk categories is based on the typical features and the rationale of the products, as listed. Firms should therefore be aware of any differences between these typical features and those of the firm’s own products, which may affect the firm’s product risks.

Due to restrictions on releasing funds, pensions and annuities are in the reduced and intermediate risk categories; however, with the rise in pension liberation, there are increasing opportunities to obtain funds from these products.

FINAL BOARD APPROVED

Firms may also develop new, innovative products, to provide an income in retirement, given that an annuity will no longer be a compulsory option, as it has been for many pension plan maturities.

In light of these changes, firms should review their transaction monitoring programmes, to ensure unusual or suspicious activity is highlighted for further investigation. Depending on a firm's product and customer risks, firms may also wish to follow the additional customer due diligence requirements in 7.39.

Intermediate risk

(i) What constitutes the outset of the business relationship?

In most cases a business relationship begins with the acceptance of a fully completed application or proposal form.

However, the business relationship is only formally established after the end of the cooling off period. This is important for the timing of customer due diligence.

(ii) What about cancellation during the "cooling-off period" leading to a refund of premium paid? In some cases, the customer has not yet been verified by that time.

Firms should seek to mitigate risk by refunding the premium to the customer by way of direct credit to the bank account from which the funds were paid or by an account payee crossed cheque in the customer's name. Firms should also consider whether the cancellation, taken into consideration with all other factors, raises suspicions about the transaction and if they do, consent must be sought from NCA before paying out the sum. Where there is no such suspicion, firms should also verify the customer's identity before making a refund where the premium is 'large' (the sectoral guidance purposely does not set a lower limit, as materiality thresholds of individual firms will differ with the different features of the product) and/or circumstances appear unusual. (Note: this requirement also applies to increased risk business).

(iii) What information do we need to obtain in respect of intermediate risk pensions to satisfy customer due diligence requirements?

Verification should be undertaken in line with the guidance in Part I paragraphs 5.3.228 to 5.3.237.

CDD can be fully satisfied with the pension scheme tax reference number, which shows the scheme is registered with HMRC. (This information should be held by product provider.)

Note - HMRC do not issue approval letters. However, if the firm has any concerns, on application and with the relevant authority, HMRC will provide documentary confirmation regarding the existence of the scheme.

If pension scheme members make direct contributions to the scheme (not via salary deduction), their identities should be verified accordingly.

If benefit payments are made to the trustees or a member of the pension scheme, additional verification will not be required if the payment is made to an account in their name at an UK or EU regulated financial institution.

If a member requests that their Tax Free Cash amount is paid to a third party, additional checks will be required, including verification of the third party.

FINAL BOARD APPROVED

Contributions from any third party not connected to the pension scheme will require the third party's identity to be verified in accordance with Part I, chapter 5.

- (iv) *What if the product provider is the trustee of the pension scheme?*

The individual members' identities need to be verified e.g., for individual personal pensions.

- (v) *Who are the relevant parties whose identity should be verified for TIPs?*

Trustees

For UK regulated financial services company trustees, only confirmation of regulatory number is required, or if funds are from a HMRC regulated scheme, the pension scheme tax reference number is sufficient.

Note - HMRC do not issue approval letters. However, if the firm has any concerns, on application and with the relevant authority, HMRC will provide documentary confirmation regarding the existence of the scheme.

- (vi) *What about verification on intermediate risk level pension transfers?*

A risk-based approach can be taken, as a firm's identification and verification obligations for the contract owner(s) may be met if the transfer is from a FCA-regulated financial services firm.

In addition to obtaining the pension scheme tax reference number (which shows the scheme is registered with HMRC), the source of funds should be identified by obtaining:

- 1 the previous pension provider's name; and
- 2 the previous scheme or plan name, its reference or PSO/PSTR number where relevant and the type of plan

Taking a risk-based approach, consideration should be given to the jurisdiction from which a Recognised Overseas Pensions Scheme originates, to determine whether any further verification of the relevant parties is required.

- (vii) *What about traded endowments?*

The trading of an endowment policy increases exposure to money laundering. A policy can be bought and sold several times before a firm necessarily becomes aware of the reassignment, usually on payout. The insurer should verify the identity of the owner at payout usually in line with the standards set out in Part I, Chapter 5. Where the transfer/s have taken place through a 'market maker' in traded endowments, and that firm is regulated by the FCA, reliance may be sought from the market maker in accordance with Part I, section 5.5.

- (ix) *What if a pension-sharing order or pension-earmarking order (for example, in the case of a divorce) is received for an intermediate risk pension?*

Firms may accept court documents as verification of identity of the existing customer, if this has not already been completed.

Subject(s) of such an order that are explicitly nominated to receive funds should be regarded

FINAL BOARD APPROVED

as the beneficial owner(s), and their identity may also be verified by reference to the court document(s).

- (x) *What if a payment on death is to be made direct to a beneficiary?*

Payments to beneficiaries on the instructions of the executor or administrator may be made once the beneficiaries have been PEP and sanction screened. If there are no PEP or sanctioned parties involved, there is no need to verify the identity of beneficiary, if the payment is made to an account in their name. However, if a beneficiary wishes to transact any business their own name, their identity will need to be verified, in line with the guidance in Part I, section 5.3 and paragraph 5.3.2.

- (xi) *Is the pensions and annuities risk increased with Pension Liberation and the UK Government's April 2014 budgetary changes, which remove the requirement to take an annuity and give easier access to pension funds?*

The placement of all products listed in this section into risk categories is based on the typical features and the rationale of the products, as listed. Firms should therefore be aware of any differences between these typical features and those of the firm's own products, which may affect the firm's product risks.

Due to restrictions on releasing funds, pensions and annuities are in the reduced and intermediate risk categories, however with the rise in pension liberation, there are increasing opportunities to obtain funds from these products.

Firms may also develop new, innovative products, to provide an income in retirement, given that an annuity will no longer be a compulsory option, as it has been for many pension plan maturities.

In light of these changes, firms should review their transaction monitoring programmes, to ensure unusual or suspicious activity is highlighted for further investigation. Depending on a firm's product and customer risks, firms may also wish to follow the additional customer due diligence requirements in 7.39.

- (xii) *Who do we verify if an intermediate product is written in trust (Beneficial Owners)*

Beneficial Owners need to be "identified". Their identity in most cases needs to be "verified" in line with the guidance in Part I, paragraphs 5.3. 8 to 5.3.13. Beneficial Owners include the trustees and also beneficiaries, who may be named individuals or a class of beneficiary.

At the outset of the business relationship firms should always seek to 'identify' and 'verify' the identity of the settlor and the trustees. Beneficiaries should always be "identified" as individuals or with a defined class, for example this can be done by requesting a copy of the trust deed* or by requesting this information from the trustee directly

In all cases, regardless of risk, if payment is made direct to a beneficiary at the request of a trustee, the identity of the beneficiary should be verified, PEP and sanction checked prior to payment being made, if this has not already been done. Where payment is being

FINAL BOARD APPROVED

made to the trustee(s), the trustee(s) should be verified, PEP and sanction check if this has not already been done.

* It is recommended that firms liaise with their legal consultants over whether or not to request a copy of the trust deed.

Increased Risk

- (i) *Who are the relevant parties for these products in terms of verification of identity?*

The relevant parties are summarised in the table below:

Savings/investments	<i>Relevant parties to be identified</i>
1 Bonds	<ul style="list-style-type: none"> ○ <i>Policy holder or applicant</i> ○ <i>All payers if different to policy holder</i> ○ <i>All payees if different to policy holder</i> ○ <i>Beneficial Owners (verification on higher risk cases – see FAQ v below)</i>
Pensions	
None	

- (ii) *What constitutes appropriate ongoing monitoring and controls?*

- a) Firms should, as part of normal commercial procedure, be considering for each product what ‘trigger points’ occur between customer entry and customer exit which might serve to increase that product’s exposure to abuse. Examples of trigger points could be early surrender of a product (‘early’ in the context of a firm’s normal business pattern for that product) or a change in payer and/or beneficiary. Appropriate transaction monitoring can then be set up.
- b) This guidance purposely avoids setting monetary thresholds for monitoring (e.g., all surrenders over a certain € amount) because materiality will differ significantly between firms. Firms should identify key indicators pertinent to their own business patterns, taking into account, for example, average premium income size per customer and average duration of the contract in force. With that qualification, suggested standard practice for each increased risk product is summarised in the table below.

Savings/investments	<i>Suggested practice for monitoring and control</i>
1 Bonds	<ul style="list-style-type: none"> ○ <i>Cancellation (i.e., applications not proceeded with after funds received)</i> ○ <i>Early surrenders (i.e., within a certain time period, which is to be specified by individual firms) over a certain € threshold</i> ○ <i>Multiple partial surrenders, totalling up to (say) 75% of original investment, within the specified time period</i> ○ <i>Top up payments over a certain € threshold (dependent on individual firms’ assessment of materiality) and frequency</i> ○ <i>Third party payments of any value</i> ○ <i>Non UK residents</i>
Pensions	

FINAL BOARD APPROVED

None

- (iii) *Additional customer information is not always readily available when business has come through an intermediary. How should we go about obtaining it?*

It is recognised that business transacted in a non face-to-face capacity, or through Financial Advisors, presents particular difficulties for insurance firms seeking to satisfy their additional information obligations under Part I, Chapter 5. Firms should, continue to obtain the limited information required via their own direct sales force (DSF) (where applicable) or, where business has come through an intermediary, should include a request for the information as part of their customer application or proposal form. Financial advisers and DSF should gather same level of data. It is suggested that the additional information required will be collected as part of an application form, and not part of the introduction certificate.

- (iv) *Do we need to obtain supporting documentation for the additional information requested from a customer?*

Verification is limited to identity only. In most circumstances, additional customer information may be taken at face value. However, if the additional information provided appears incongruous or contradictory, this should serve to raise suspicions about the transaction and firms are then expected to make further enquiries which may in some circumstances involve seeking documentary support to the additional information.

- (v) *Who do we verify if a Bond is written in trust (Beneficial Owners)*

Beneficial Owners need to be “identified”. Their identity in most cases needs to be “verified” in line with the guidance in Part I, paragraphs 5.3.8 to 5.3.13. Beneficial Owners include the trustees and also beneficiaries, who may be named individuals or a class of beneficiary.

At the outset of the business relationship firms should always seek to ‘identify’ and ‘verify’ the identity of the settlor and the trustees. Beneficiaries should always be “identified” as individuals or with a defined class, for example this can be done by requesting a copy of the trust deed* or by requesting this information from the trustee directly

In all cases, regardless of risk, if payment is made direct to a beneficiary at the request of a trustee, the identity of the beneficiary should be verified, PEP and sanction checked prior to payment being made, if this has not already been done. Where payment is being made to the trustee(s), the trustee(s) should be verified, PEP and sanction check if this has not already been done.

** We recommend firms liaise with their legal consultants, over whether or not to request a copy of the trust deed.*

- (vi) *How does using the “source of funds” as evidence affect increased risk level products?*

The source of funds should not be used as evidence of identity in respect of increased risk level products. However, where a firm’s own, branded version of these generic products have features which reduce the indicative risk, it may conclude that its own product falls within the “intermediate” category of risk and follow the guidance given in respect of intermediate risk products.

- (vii) *What about Power of Attorney arrangements for these products?*

Where any party requiring verification is represented by an individual or firm appointed under

FINAL BOARD APPROVED

a Power of Attorney, the identity of the Attorney should also be verified using the principles established in Part I, paragraphs 5.3.99-5.3.101.

- (viii) *What about cancellation during the “cooling-off period” leading to a refund of premium paid? In some cases, the customer has not yet been verified by that time.*

Firms should seek to mitigate risk by refunding the premium to the customer by way of direct credit to the bank account from which the funds were paid or by an account payee crossed cheque in the customer’s name. Firms should also consider whether the cancellation, taken into consideration with all other factors, raises suspicions about the transaction and if they do, consent should be sought from NCA before paying out the sum. Where there is no such suspicion, firms should also verify the customer’s identity before making a refund where the premium is ‘large’ (the sectoral guidance purposely does not set a lower limit, as materiality thresholds of individual firms will differ with the different features of the product) and/or circumstances appear unusual.

Where funds have derived from a building society cheque or bankers’ draft, the money cannot be returned to source. Firms may therefore wish to seek that the account to which the customer requests their funds are returned, is an established account in the firm’s customers name, with a regulated financial institution. For example a bank statement could be requested as evidence.

- (ix) *What if a payment on death is to be made direct to a beneficiary?*

Should executors or administrators instruct payments to be made directly to the beneficiaries, the identity of the beneficiaries should be verified, if not already done so, in line with the guidance in Part I, paragraphs 5.3.8 to 5.3.13, prior to the payment being made. Sanction and PEP checks should also be undertaken.

7A: General insurers

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Introduction

- 7A.1 The intention of this guidance is to provide clarification for General Insurers as to their obligation to report suspicious activity under the Proceeds of Crime Act 2002 (POCA), comply with sanctions legislation and explain the new powers granted to H.M. Treasury under the Counter Terrorism Act 2008. General Insurers are not within the regulated sector, as defined under the Money Laundering Regulations 2017, but in certain circumstances they are required to report suspicious activity to the National Crime Agency (NCA).
- 7A.2 Part 7 of POCA came into force on 24 February 2003. This sectoral guidance focuses on the obligations of general insurers and is designed to assist General Insurers in applying legislation consistently. The objective is to help general insurers refine their current practices and to identify whether they are complying with POCA.
- 7A.3 This guidance is not a replacement for detailed advice on specific activities and problems and it should not be regarded as a substitute for legal advice on any of the topics discussed. General insurers should, periodically, seek their own legal advice to ensure that their understanding of the legal framework is up to date.

Proceeds of Crime Act and the Terrorism Act

- 7A.4 The offences under POCA and the Terrorism Act relate to any activity involving criminal or terrorist property (including, sometimes, the criminal or terrorist act itself). This is a much broader definition than the commonly understood definition of money laundering (i.e., the movement, layering and concealment of criminal funds). A company, for example, can commit an offence under POCA by unwittingly facilitating an act of fraud.
- 7A.5 Obligations under POCA and the Terrorism Act, in practical terms, vary depending on which sector is seeking to apply them. General insurance is considered to be a low risk sector for both money laundering and the concealment or conversion of the proceeds of crime. General insurance is regarded as being at greater risk from fraudulent claims, rather than as a conduit for the proceeds of crime or money laundering. The majority of general insurance products do not, per se, offer obvious scope to be of use to money launderers. There is, however, scope for insurers to become unwittingly involved in criminal offences such as fraudulent claims or deliberately providing inaccurate information at inception, which may trigger provisions under POCA for suspicion reporting.

Risk-based approach

- 7A.6 The guidance on money laundering prevention in Part I, addressed to the wider financial sector is risk-based. It is recommended that general insurers also adopt a risk-based approach to their obligations under POCA and the Terrorism Act 2000.
- 7A.7 The implementation of risk management can be a simple process depending on the range of products on offer and should be linked to the profile of the customer. Insurers who also offer life products will already be aware of the requirement to carry out Customer Due Diligence (CDD). A general insurer is not required to seek the equivalent level of information on their customers, but it

FINAL BOARD APPROVED

is recommended that risk management be considered by non-life insurers at the earliest possible stage e.g., when a potential customer makes an approach or when a broker advises the insurer of a new customer, as well as when policies are renewed or claims are submitted, based on the information an insurer has. It requires the full commitment and support of senior management and the active co-operation across business units.

7A.8 General Insurers are advised to set a policy in relation to meeting their obligations under POCA and the Terrorism Act that is disseminated consistently across the company. Senior management needs to support internal policies, procedures and controls.

7A.9 General insurers should consider the following:

- Development of internal policies and procedures;
- Communication of those policies and procedures to all staff;
- Clear and written procedures in place to help staff identify the kinds of activities or customers that might arouse suspicion;
- Clear guidance to be given to all staff on the risk and implications of alerting potential or actual customers (or agents thereof) to the fact that a SAR has been submitted i.e. the "tipping off" provision of POCA;
- Clear guidance to be given to all staff on the risk and implications of failing to report their suspicions,
- Short reporting lines between front-line staff and a nominated officer;
- Record keeping: both of decisions made in the event of a suspicious claim being reported to evidence the making of the report and, in the event of a SAR not being made, the reasons why no notification was made;
- Screening procedures to ensure high standards on recruitment.
- Ongoing employee training to ensure employees recognise suspicious activities and understand the procedure in place internally to record suspicious activities;
- A system of testing compliance: this should be both independent and adequately resourced.
- Although not a regulatory requirement, the appointment of one or more nominated officers responsible for assessment of internal suspicious activity reports and engaging with the NCA, or other appropriate agencies, in respect of reporting obligations.

Reporting Suspicious Activity

7A.10 The main occasions when the requirements under the POCA will apply to general insurers is during underwriting and when processing claims. Nothing in POCA prevents the underwriter or claims handler from properly challenging the information supplied by the customer. Information available to an insurer when processing a claim is limited, and the claimant usually controls access to this information. The job of a underwriter / claims handler is in part to establish the facts of the potential business / claim.

7A.11 The offences in POCA relate to money laundering rather than attempted fraud. Paragraphs 6.43 – 6.47 in Part I of the JMLSG guidance specify when attempted frauds need to be reported to the NCA. Thus, the General insurer has to know or suspect, or have reasonable grounds to know or suspect, that there has been some benefit obtained by the fraudster, as the benefit represents criminal property.

7A.12 During the claims process there may be suspicion on the part of a member of the claims team that the customer may be embellishing their claim and there may be a number of challenges and procedures that will be followed until the claim is agreed or declined. Whilst this process is ongoing the customer may be attempting to commit a fraud, but this is not a reportable offence under POCA.

FINAL BOARD APPROVED

- 7A.13 However, if a claim has been accepted and agreed and the insurer has paid the claim and subsequently it is discovered that there are reasonable grounds to know or suspect that the claim was false, then the reporting provisions under POCA are met and the insurer must file a suspicious activity report (SAR) with the NCA as soon as practicable. This is because any payment made as a result of the claim is now classified as criminal property and must be reported to the NCA.
- 7A.14 General insurers do not have an obligation to appoint a nominated officer to deal with disclosures of SARs. However, POCA applies to both regulated and unregulated sectors and SARs can be made to the NCA by any industry representative. If insurance firms elect to appoint a single point of contact who would be regarded as a nominated officer, there are additional obligations in respect of reporting to the NCA and where consent may be required, after an internal report is made to him/her. In practice, this means an obligation to submit a SAR (see Part I, Chapter 6). Failure to do so may mean he/she will commit an offence under section 332 of POCA. From a practical perspective it is advisable for someone to coordinate a company's anti-money laundering procedures as well as administer obligations under POCA. This would give staff a contact that they can approach if they have any suspicions.
- 7A.15 If there is no nominated officer, employees should make disclosures to the NCA by way of a SAR. SARs can be submitted electronically or by post though the NCA is actively encouraging the use of the SAR Online system which can be found at www.nca.gov.uk.

Financial Sanctions

- 7A.17 Under the financial sanctions regime it is a criminal offence to make either funds or financial services available to the targets on the Financial Sanctions Consolidated List which are published and maintained by the Office of Financial Sanctions Implementation (OFSI). Financial sanctions apply to all companies, irrespective of whether or not they are regulated. The guidance contained in Part I, paragraphs 5.3.54- 65, and Part III should be followed.
- 7A.18 Financial sanctions apply to all forms of payment and services offered. In respect of General Insurers this applies not only to the contract of insurance but could also apply to third party payments and providing replacement vehicles and articles. In relation to proliferation financing, the provision of insurance cover to shipments of goods which contravene related export controls could cause the insurer (or broker) to breach relevant legal and/or regulatory obligations. See Part II, sector 15: *Trade finance*, especially paragraph 15.28 and Annex 15-IV.
- 7A.19 General Insurers will also have to consider how their partners and brokers, including outsourcers, are mitigating this risk and who is responsible for ensuring that some form of monitoring is being undertaken to prevent payment to any listed person or entity.

Counter Terrorism Act 2008

- 7A.20 The Counter Terrorism Act was enacted on the 26th November 2008 and introduces additional obligations on firms in the fight against money laundering, terrorist financing and the proliferation of nuclear, radiological, biological or chemical weapons. Directions under this act can only be given by HM Treasury.
- 7A.21 There are four specific instances where this Act may be used but only two of the directions may be given to General Insurers. These are the directions in respect of **systematic reporting**, where a direction may require a firm to provide such information and documents as may be specified in the direction relating to transactions and relationships with designated persons. The direction will specify to whom the information and documents are to be provided and the period within or the intervals at which they are to be provided.

FINAL BOARD APPROVED

- 7A.22 The second direction relates to **limiting or ceasing business**. Such a direction may require a firm not to enter into or continue to participate in a specified transaction or specified description of transactions or business relationships with a designated person or any transaction or business relationship with a designated person.
- 7A.23 Part I, section 5.8 provides further guidance on meeting obligations imposed under these directions.

8: Non-life providers of investment fund products

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Where a firm offers investment products as described in both this section and in Sector 7, for which the levels of risk are similar, it may wish to refer to Sector 7 from paragraph 7.51 onwards when dealing with all these products.

Overview of the Sector

8.1 The guidance contained within this section is directed at firms offering the following types of investment vehicle:

- (a) *Retail investment funds* - authorised unit trusts and open-ended investment companies (OEICs).
- (b) *Other investment fund-based products/services* - which may comprise one, or a combination of, regular savings schemes (including those relating to investment trusts), regular withdrawal schemes, ISAs, personal pension schemes and fund supermarkets.

Typical investors using retail funds and associated products/services vary depending upon the product, but include private individuals, regulated firms investing as principal (e.g. life companies); other regulated firms (including nominee company subsidiaries) acting on behalf of underlying customers, other corporates, personal and corporate occupational pension schemes, charities and other trusts.

- (c) *Institutional funds* - authorised and unauthorised collective investment schemes and unitised life assurance funds that are dedicated to investment by institutional investors.

Investment in such funds is often restricted to UK investors who are exempt from taxation on capital gains - principally HMRC approved pension schemes and charities.

8.2 For most firms, investors will be mainly, but not exclusively, UK resident.

8.3 This section does not aim to provide guidance to life assurance companies, other than for the purposes of providing institutional funds as described in paragraph 8.1(c). In addition, it does not cover the issuance or trading of shares in closed-ended investment vehicles (e.g. investment trusts). Guidance on other life assurance products can be found in Sector 7: *Life assurance and life- related pensions and investment products*. The issuance and trading of shares in investment trusts etc.

FINAL BOARD APPROVED

fall within the scope of Sector 14: *Corporate finance* and Sector 10: *Execution-only stockbroking*, respectively.

- 8.4 Guidance for those involved in managing private equity funds is contained within Sector 13: *Private equity*.

The money laundering risks relating to investment fund products

Risk Based Approach

- 8.5 As outlined in Part I Chapter 4, all firms must develop a risk based approach to mitigating the risk of their products and services being used for the purposes of money laundering or terrorist financing. Firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms should have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk.
- 8.6 Firms should assess the risk of the products they provide, the services they offer and the relationships that they have with their customer. Where a low degree of risk is determined then Simplified Due Diligence (SDD) may be applied. Where a high risk is identified then Enhanced Due Diligence (EDD) measures should be applied; in other circumstances, standard Customer Due Diligence (CDD) will apply.

Retail funds

Product/Service Characteristics

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Third party payers/subscribers which could disguise the source or destination of laundered funds.	As a general rule third party payments are not accepted unless made to/from another regulated entity.	Monitoring will identify exceptions which will be reviewed and, where necessary, appropriate due diligence measures will be performed on the third party.	Low
Ability to pay in or withdraw cash	No receipt or payment in cash is possible	No receipt or payment in cash is possible.	Low
Ability to switch from one product to another	Products allow switching between funds but the registered owner remains the same	Monitoring will alert to any unusual behaviour.	Low
Ability to transfer holdings to a third party to try and mask the audit trail	Products allow stock transfers to enable registration under and alternative name	Transfer is often to another regulated entity. Appropriate due diligence is performed on the new client. Monitoring will alert to any unusual behaviour.	Low
Products which enable high turnover of funds	Generally products tend to be simple and many provide for tax-exempt investment.	Types of funds The following are deemed to be low risk products:- <ul style="list-style-type: none"> • ISAs • JISAs • LISAs Complex products that allow a high turnover of funds may increase the risk, for example, <ul style="list-style-type: none"> • Real Estate Funds • Structured Finance • Liquidity Funds 	Low Medium

Transactions

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Transaction activity is high in value	This can differ dependant on the client profile.	Platform/distributor business can be large in value but these are other regulated firms. Private clients investing up to £50,000 may be considered to be low risk, which enables the source of funds to be used as evidence, so applying (SDD). Monitoring identifies suspicious transactions	Low Low
Transaction activity is high in volume	This can differ dependant on the client profile.	Platform/distributor business can have high volumes of trading as they represent their underlying investors, but these are other regulated firms. Private clients tend to invest for the medium to long term and therefore transact less frequently. Monitoring should identify any unusual trading patterns.	Low Low

Client Characteristics

Risk Factor	Inherent risk	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Complex ownership structures, which can make it easier to conceal underlying beneficiaries	Medium	Clients are largely the subject of some form of regulation or private individuals where the legal and beneficial owner is easily identifiable	CDD is performed on the client and any beneficial owners, where required.	Low
Request to use numbered accounts or "hold mail"	Medium	No anonymous accounts allowed. Mail is held for Gone Away clients	CDD is performed at the point of contact, on a risk sensitive basis.	Low
Nature and scope of client's own business (e.g. cash intensive)	Medium	Not considered applicable to this sector of the industry		
Customers represented by a third party	Medium	These tend to be subject to court approval or ratification (e.g. Executors and POA Attorneys)	Evidence of official appointment obtained In the case of Attorneys who are appointed under powers of attorney, firms may identify and verify all attorneys	Low
Purpose of investing	Low	It may be assumed that most investors investing in retail funds will be doing so for the investment returns	Firms should, on a risk based approach, ask for additional information about the purpose of the relationship, where this is appropriate	Low
Involvement of an individual in a prominent public position (PEP/RCA)	High	It is possible that the client could be a PEP or family member or close associate of a PEP	Regular screening of public source information (e.g. World-check, Dow Jones). Enhanced CDD performed	High

Delivery Channels

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Ability to transact non face-to-face	Transactions can be placed in writing, by phone, post or by a platform, distributor or intermediary.	Platform, distributor, intermediary business involves other regulated firms. Private clients are subjected to additional CDD measures (e.g. certification of documents).	Low

FINAL BOARD APPROVED

Correspondent relationships (where applicable)	Relationships are predominantly with EU firms	Increased level of CDD to include an assessment of the third party's systems and controls (e.g. Wolfsburg Questionnaire).	Medium
--	---	---	--------

Geography

Much of the risk assessment mentioned above will be dependent upon the jurisdiction the client is domiciled. Firms will take note of their own internal country risk assessment which will be driven by assessments and information provided by Government, Regulators and other relevant authorities. Where the risk dictates, increased measures will be taken to mitigate the ML/TF risk.

Where a client originally invests in the UK and subsequently moves abroad to a high risk country, this does not necessarily in itself lead firms to believe this is a high risk customer unless there are other factors present (e.g., PEP status, funds received from or paid to a bank account in a high risk country).

- 8.7 On balance, therefore, investment funds and products that involve the restrictions controls referred to above may generally be considered to be low risk in terms of their use for money laundering purposes. However, if the features of a product or service provide additional flexibility (for example, where some or all of the risk mitigations referred to in the table following paragraph 8.6 are not applied), the firm should consider the potential increase in the money laundering risk given all the relevant factors and the need to mitigate that risk.

Institutional funds

- 8.8 Many institutional funds are open only to tax-exempt investors, such as pension schemes and charities.
- 8.9 As with retail funds, investors are rarely asked to provide additional customer information. However, in many cases the investment will be made on behalf of a customer by the firm itself, another group company or another regulated firm, who will have obtained such information in the context of their role as an investment manager.
- 8.10 Overall, the majority of institutional funds business may be considered to be of lower risk than their retail counterparts, by virtue of the restricted types of investor, many of whom are themselves regulated, rather than because of the product's features. The risk will increase, however, in the case of "non-exempt" funds or share classes, which may admit other types of UK and non-UK institutional investor that are not subject to HMRC approval for tax exemption purposes.

Defining the customer for AML purposes

- 8.11 The Money Laundering Regulations 2017 define a "business relationship" to include any business, professional or commercial relationship between the firm and its customer, which is expected to have an element of duration. Essentially, this definition would apply to any open-ended product relationship (e.g. managing an ISA), irrespective of whether it was for the purposes of lump sum or regular investment. Furthermore, a fund manager's obligation to redeem units at the request of the holder at some future time provides the relationship and element of duration necessary for the definition to apply in the case of any registered holder of units, however their holding was acquired.

FINAL BOARD APPROVED

- 8.12 The handling of third party payments is an important feature of the typical risk profile of the fund management sector. Where the firm accepts payment from a third party at any point, that party should also be regarded as a customer and verified as such.
- 8.13 Should an investor ask a firm to pay redemption proceeds to a third party, that third party should also be regarded as a customer (on whose behalf the registered investor may have been acting), and their identity should be verified on a risk based approach, before any funds are remitted. In instances where the beneficial owner remains the same, then this can be treated as lower risk.
- 8.14 As stated in the ESA Risk Factor Guidelines firms may generally treat platforms/fund supermarkets as their customer, and not have to ‘look through’ them to the underlying investor.
- 8.15 Customer Due Diligence measures should remain limited to identifying and verifying the identity of the Intermediary and to verifying that the Intermediary has a robust and risk sensitive AML program in place and applies Customer Due Diligence measures to its customers and to its customers’ beneficial owners.
- 8.16 Firms are not required to assume that payment from an unidentified source (e.g. by wire transfer from a UK bank or building society cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be, the case.

Customer Due Diligence***Identity verification measures***

- 8.17 Standard verification procedures for the type of customer concerned, and any beneficial owner or controller, as described in Part I, Chapter 5, should be followed. Subject to the restrictions that apply generally to their use, various modifications to standard procedures are available. Typically, these would include:
- (i) application of simplified due diligence in relation to customers or products determined as presenting a low degree of risk, as described in Part I, Chapter 5;
 - (ii) use of the source of funds as evidence of identity - see Part I, paragraphs 5.3.102 to 5.3.107 (firms should limit its use to lowest risk cases, and in any case should not use it where the value exceeds £50,000).
 - (iii) application of the measures described in Part I, paragraphs 5.3.95-5.3.98 in relation to the administration of deceased investors and Court of Protection Orders.
- 8.18 Where the firm is required to verify the identity of a customer that is being introduced by an appropriately regulated intermediary (see Part I, paragraph 5.6.11-5.6.18), reliance may be placed on the intermediary, following the guidance in Part I, paragraphs 5.6.19ff.

FINAL BOARD APPROVED

- 8.19 In the case of beneficial owners or controllers, unless the relationship is higher risk (by virtue of the services to be provided or the specific nature of the customer), the identity of beneficial owners and controllers may be confirmed by the customer themselves (see Part I, paragraphs 5.3.8 to 5.3.13).
- 8.20 Knowledge that the customer(s) is/are acting in a trustee capacity and identification of the beneficial owners does not mean that a firm has accepted or recorded notice of trust or otherwise make the firm a constructive trustee.
- 8.21 Various types of small occupational pension scheme may invest in retail funds - in cases where Simplified Due Diligence cannot be applied the verification procedures described in Part I, paragraphs 5.3.228 to 5.3.237 should be followed. Where the customer is a UK-based personal pension scheme (e.g. a SIPP), however, the firm should confirm that any third party trustee or administrator that may deal with the firm has been appointed by the regulated scheme operator. This will be a factor to be considered by the firm when determining whether to apply simplified due diligence to such customers.
- 8.22 As most business within this sector is conducted non-face-to-face, consideration needs to be given to the higher money laundering risk this may present compared with face-to-face business, and in particular whether or not the person with whom the firm is dealing may be impersonating someone else. Given the lower risk of this sector being used for money laundering purposes, the usual measure taken in this respect is to ensure that the confirmation of a transaction or acknowledgement letter is sent by post to the customer's known address and is not returned or queried by the occupant.

Firms with legacy customers whose identity has not been verified due to the circumstances under which they became investors, and for whom the firm is unable to return the funds, are not expected to undertake specific exercises or projects to verify the identities of those customers retrospectively, but must do so upon future trigger events, as appropriate according to their risk-based approach.

Additional customer information

- 8.23 Additional customer information over and above that confirming identity, which is appropriate in many sectors, either for business purposes or because of the greater money laundering risks that their products and services entail, may be less useful in this sector for managing financial crime risk, for reasons articulated above. While firms should request further information, on a risk based approach, from an AML/CTF perspective, the principal objective in obtaining such information is to understand the motive for establishing the relationship and to permit assessment of any subsequent activity. The motive for investing in funds is usually self-evident: if it is anything other than medium to long-term investment returns then the objective should be recorded and taken into account in assessing the risk of the relationship.
- 8.24 High risk relationships (e.g. politically exposed persons (PEPs), high value accounts or account holders associated with higher-risk territories), should, however, be treated with caution. Firms should give due consideration to the nature and purpose of the relationship by obtaining more information concerning the customer's rationale for using its services and demonstrating their source of wealth.

FINAL BOARD APPROVED

- 8.25 Furthermore, firms will need to take a risk-based approach in identifying a customer's potential status as a PEP. Firms are required to take risk-based steps to determining PEP status, where the money laundering risk is higher - depending, for example, on the value of the investment and/or the location of the customer.
- 8.26 Activity monitoring of retail investment investors can be equally, if not more, effective by comparing the behaviour of one customer with that of others (see paragraphs 8.36 – 8.39).
- 8.27 Care should also be exercised when dealing with those claiming the reduced verification measures applicable to certain types of special cases (e.g. asylum seekers, those on low incomes), whose first priority would not be expected to be investment of their limited resources for the future (see Part I, paragraph 5.3.87).

Timing of verification

- 8.28 The obligation to verify a customer arises at the point when it is clear that they wish to enter into an arrangement with the firm, either to buy or sell units in a fund or to establish some form of investment scheme or account. In addition, given the revised definition of "business relationship" (see paragraph 8.11) the transfer of units from an existing holder to a third party will also give rise to an obligation to verify the identity of the transferee.
- 8.29 Firms must verify a customer's identity as soon as practicable after first contact with the customer, but are not prevented from entering into the relationship or commencing the initial transaction before the checks are completed. Firms should take all reasonable steps to verify the customer's identity within a reasonable time. Where the firm is unable to verify the identity of the investor within that time it will cease proactive pursuit of evidence of identity and must, at that point, consider if the circumstances give any grounds to suspect money laundering or terrorist financing and act accordingly (see Part I, paragraph 5.2.8).
- 8.30 If, however, after such reasonable time the firm has no grounds to suspect and is satisfied that the risk of money laundering is minimal, subject to its terms of business or the status of a contract to purchase units in its funds directly, it may terminate the relationship and return any monies received to their source. Alternatively, and particularly in purchases of units where the contract has been completed, the firm should freeze any funds or assets pending eventual verification (see Part I, paragraph 5.2.9).
- 8.31 From the point at which the firm ceases proactive pursuit of evidence of identity, (either without suspicions or requesting consent from NCA to terminate), it must *freeze* an investment:
- (a) it must not accept further investments (ad hoc or regular savings) from the customer until they provide the evidence of identity required by the firm;
 - (b) it must permit the investor to withdraw, redeem or transfer their investment upon production of the evidence of identity required by the firm;

FINAL BOARD APPROVED

- (c) it should otherwise continue to act in accordance with any relevant terms of business and regulatory obligations until such time as the relationship may be terminated (this would include issuing periodic statements, making normal dividend/interest payments and administering the customer's investments according to their instructions where these do not involve the investment or withdrawal of capital); and
- (d) it must take steps to remind customers (individually or generically, as appropriate according to their risk-based approach) that evidence of identity may still be required, noting the consequences of failure to comply with the firm's request.

8.32 From the point at which a firm submits a SAR, until it receives such consent, it must:

- adhere to bullet points (a)-(d) above; and
- desist from continuing to apply Customer Due Diligence measures in relation to that customer,

where that would result in the commission of an offence under-

- (i) section 21D of the Terrorism Act 2000 (tipping off: regulated sector)(a); or
- (ii) section 333A of the Proceeds of Crime Act 2002 (tipping off: regulated sector)(b).

8.33 A customer may wish to redeem their investment or exercise a right to cancel a purchase transaction before the firm has been able to verify their identity. In such circumstances, the firm should consider whether or not the circumstances might suggest grounds for suspicion of money laundering or terrorist financing and a need to submit a SAR seeking a defence to money laundering from NCA, before returning any funds to the customer (see also paragraph 8.38 below).

8.34 Firms should exercise caution in the event that a holder seeks to transfer units to someone else before the firm has been able to verify their identity. This will either be soon after the units were acquired and while the firm is still attempting to verify the transferor, or where the firm has frozen the investment having been unable to complete satisfactory customer due diligence and not received consent on submitting a SAR.

8.35 Firms are recommended to include in their terms of business, or otherwise advise the customer at the outset, that they may return or freeze the customer's investments unless or until the necessary evidence of identity can be obtained.

Monitoring

8.36 As mentioned in paragraph 8.26, one of the most effective ways of monitoring the activity of an investor is to compare it with that of the "typical investor". This may vary for different types of customer (e.g. private individual compared to a corporate investor) and also for different types of fund (e.g. money market fund compared to an equity fund).

FINAL BOARD APPROVED

- 8.37 Other than in the case of regular savings/withdrawal schemes, the use of investment funds and products is by its nature ad hoc. Even with regular savings and withdrawal schemes, however, there is nothing unusual in ad hoc additional, or top-up, subscriptions. However, whilst there may be various legitimate reasons for redeeming an investment after a relatively short period of time, most retail investment is made for the medium to long-term.
- 8.38 As such, firms in this sector will place some reliance upon the alertness and experience of its staff to spot unusual activity. However, firms may also consider the implementation of basic exception reporting to identify, for example, short-term investment by individuals. Disposals so identified might be reviewed in the context of the original purchase (e.g. is it within the charge-back period for a subscription by debit card?) against market conditions, or in the light of any specific information the firm has about the investor. The exercise of cancellation rights is relatively rare and should be considered in a similar way.
- 8.39 Transfers involving either a regulated firm (or a nominee company subsidiary) or arising from the distribution of assets from a trust or the estate of a deceased, give less cause for concern over a subsequent transfer of the holding by the recipient. However, the purchase of units by one individual and transfer to another, and then to a third, and so on, is unusual and may indicate that money or other consideration is changing hands in the background with the aim of avoiding verification of the identity of those in the middle of the chain. Firms should be alert to such activity and take appropriate steps to investigate the nature and purpose of any unusual patterns that emerge.

9: Discretionary and advisory investment management

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the Sector

- 9.1 *Investment management* includes both discretionary and advisory management of segregated portfolios of assets (securities, derivatives, cash, property etc.) for the firm's customers. Where investment management is provided as part of a broader "wealth management" service, readers should refer instead to Sector 5: *Wealth Management*.
- 9.2 Discretionary managers are given powers to decide upon stock selection and to undertake transactions within the portfolio as necessary, according to an investment mandate agreed between the firm and the customer.
- 9.3 Advisory relationships differ, in that, having determined the appropriate stock selection, the manager has no power to deal without the customer's authority - in some cases the customer will execute their own transactions in light of the manager's advice. This should not be confused with "financial advice", which involves advising customers on their investment needs (typically for long-term savings and pension provision) and selecting the appropriate products. Financial advice is dealt with in Sector 6: *Financial advisers*.
- 9.4 The activities referred to above may be carried out for private or institutional investors. Note that guidance on the operation of investment funds, including those that are solely for institutional investors, is given in Sector 8: *Non-life providers of investment fund products*.

What are the money laundering risks relating to investment management?

- 9.5 In terms of money laundering risk, there is little difference between discretionary and advisory investment management. In both cases, the firm may itself physically handle incoming or outgoing funds, or it may be done entirely by the customer's custodian.
- 9.6 In either case, the typical firm deals with low volumes of high value customers, for which there should be a take-on process that involves a level of understanding of the customer's circumstances, needs and priorities and anticipated inflows and outflows of funds, in order to determine suitable investment parameters.
- 9.7 Firms should maintain ongoing contact, often face-to-face, with the customer in order to review market developments and performance, and review the customer's circumstances, etc. Unexpected inflows/outflows of funds are not common occurrences - ad hoc requirements and movements are usually the subject of discussion between the firm and the customer.

FINAL BOARD APPROVED

- 9.8 In most cases, all money and other assets within the portfolio are held under the control of a regulated custodian, with money paid to or from the customer through their bank or building society account. Investment management is not a mechanism for the movement of assets from one person to another, although some third party payments may be made (e.g. in the case of private customers, for the payment of school fees).
- 9.9 The risk of money laundering to the investment management sector, in the context of the "typical" circumstances described above, would be low. Clearly, however, the risk will increase when dealing with certain types of customer, such as:
- offshore trusts/companies,
 - higher-risk PEPs and
 - customers from higher risk countries,
 - other service features that a firm offers to its customers.

Note: Firms that provide investment management alongside banking facilities and other complex services should refer to Sector 5: *Wealth Management*.

Risk Based Approach

- 9.10 As outlined in Part I Chapter 4, all firms must develop a risk based approach to mitigating the risk of their products and services being used for the purposes of money laundering or terrorist financing. Firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms should have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk.
- 9.11 Firms should assess the risk of the products they provide, the services they offer and the relationships that they have with their customer. Where a low degree of risk is determined then Simplified Due Diligence (SDD) may be applied. Where a high risk is identified then Enhanced Due Diligence (EDD) measures should be applied; in other circumstances, standard Customer Due Diligence (CDD) will apply.

Product/Service Characteristics

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Changes to strategy or agreements.	Generally, any changes to discretionary or advisory investment management will be fully discussed between the firm and the client	Amendments to agreements are approved by those persons authorized to give authority.	Low
Third party payers/subscribers which could disguise the source or destination of laundered funds.	As a general rule third party Receipts and payments are not accepted unless made to/from another regulated entity e.g. previous manager.	Monitoring will identify exceptions which will be reviewed and, where necessary, CDD will be performed on the third party.	Low

Client Characteristics

Risk Factor	Inherent risk	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Complex ownership structures, which can make it easier to conceal underlying beneficiaries	Medium	Clients are largely the subject of some form of regulation or are occupational pension funds and large charities.	CDD is performed on the client and any beneficial owners, where required.	Low
Customers represented by a third party	Medium	These tend to be subject to regulated custodians or administrators.	Evidence of official appointment obtained	Low
Involvement of an individual in a public position (PEP/RCA)	High	It is possible that the client could be a PEP or family member or or close associate of a PEP	Screening of public source information (e.g. World-check, Dow Jones). Enhanced CDD performed	High

Transactions

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Transaction activity is high in value	This is generally the norm with discretionary and advisory investment management. This can differ dependant on the client profile.	Transaction inflows and outflows will be discussed with and notified to the appointed client manager in advance.	Low
Transaction activity is high in volume	This can differ dependant on the client profile.	Monitoring will identify any unusual trading patterns.	Low

Delivery Channels

Risk Factor	Industry Standard	Risk Mitigation	Risk Rating after mitigation
Ability to transact face-to-face	Clients will have an appointed client manager.	Regular contact between the client manager and the client will largely be on a regular basis.	Low

Geography

Much of the risk assessment mentioned above will be dependent upon the jurisdiction in which the client is domiciled. Firms will take note of their own internal country risk assessment which will be driven by assessments and information provided by Government, Regulators and other relevant authorities. Where the risk dictates, increased measures will be taken to mitigate the ML/TF risk.

Who is the customer for AML purposes?

- 9.12 The typical investors to whom investment managers provide services are high net worth individuals, trusts, companies, government bodies and other investing institutions such as pension schemes, charities and open/closed-ended pooled investment vehicles. In such cases, the firm's customer will be the individual or entity concerned. The firm must also consider whether there are any beneficial owners or controllers.
- 9.13 Firms may also be contracted to provide investment management services to other appropriately regulated UK and overseas firms in respect of their own investments (e.g. life companies) or assets they are managing for others - in either instance the investment manager's customer will be the other regulated firm, in which case the firm

FINAL BOARD APPROVED

should determine the need to consider any underlying beneficial ownership or control on a risk based approach.

Customer due diligence***Verification of identity***

- 9.14 As noted above, investment management, in itself as a service, would generally be considered as low risk, although certain investment types (e.g. real estate, infrastructure, corporate debt etc.) may represent a higher risk. In the absence of any features regarding the customer or service provided that are adjudged to increase the risk, standard identity verification measures, as set out in Part I, paragraphs 5.3.57 to 5.3.272, may be applied. Where the relationship is intermediated through a regulated adviser (e.g. financial adviser or consulting actuary), confirmation of the customer's identity by the regulated intermediary, similar to that provided at Part I, Annex 5- II, may take place.

Private individuals

- 9.15 The standard verification requirements for private individuals would be adequate to establish their identity, as described in Part I, paragraphs 5.3.57 – 5.3.105. The source of funds may also be used as evidence of identity (see Part I, paragraphs 5.3.82 – 5.3.87), subject to the restrictions that apply generally to its use. However, the firm must also adopt enhanced measures, as necessary, in respect of higher-risk categories of customer (e.g. PEPs) and jurisdiction.

Customers other than private individuals

- 9.16 When dealing with other types of customer, firms would normally be able to rely on the standard verification measures, including simplified due diligence for qualifying customers, as described in Part I, paragraphs 5.3.106 – 5.3.272.
- 9.17 For overseas pension schemes and charities, additional verification steps may be required, depending upon the risk associated with the type of customer and their location (e.g. in a higher risk jurisdiction).
- 9.18 For most charities, the firm will be able to regard those that may benefit from the charity as a class of beneficiary. As such, they do not need to be identified and verified individually. The members of occupational pensions schemes that do not qualify for simplified due diligence may be treated similarly.
- 9.19 In instances where the identities of beneficial owners or controllers must be verified individually, this may be done in accordance with Part I, paragraphs 5.3.8 - 5.3.13. If the circumstances of the relationship indicate that it is low risk (by virtue of the services to be provided or the specific nature of the customer), the identity of beneficial owners and controllers may be confirmed by the customer itself (see Part I, paragraphs 5.3.11 and 5.3.12). If CDD or EDD is to be applied then independent verification should be sought.

Mandates relating to third party investment vehicles

FINAL BOARD APPROVED

- 9.20 Some investment managers provide services to third party investment vehicles (e.g. hedge funds), which may be open or closed ended. Those firms must consider whether or not there is a need for them to look at the underlying investors in such vehicles. This will depend on the status of the vehicle and how it is operated in terms of dealing in its units/shares:
- ☐ Where such dealings are handled by an appropriately regulated entity (e.g. fund manager or transfer agent) or are traded on a regulated market or exchange, the investment manager does not need to be concerned with the underlying investors.
 - ☐ If a vehicle operates under less stringent conditions than those described above, the firm may take a risk-based approach and ensure that it is satisfied, on an ongoing basis, with the checks that are carried out by whoever controls entry to the vehicle's register of holders, and the information that will be available to the firm if required. Otherwise the firm will need to undertake its own risk-based customer due diligence, as necessary.
- 9.21 In any event, the firm must carry out appropriate due diligence on third party investment vehicles to establish and verify their form, status, purpose, and the identity of any persons who are in positions of control.
- 9.22 In most cases, the investors in such funds would be regarded as a class of beneficiary and so would not need to be verified individually. However, where the vehicle is being operated for "private" use by a specific group of individuals, verification of their identities as beneficial owners/controllers should be undertaken in accordance with the guidance given in Part I, paragraphs 5.3.8 - 5.3.13.
- 9.23 Investment management firms which provide services to unregulated vehicles such as hedge funds will find it helpful also to refer to Sector 20: *Brokerage services to funds*.

Custody and third party payments/transfers

- 9.24 Where, money or investments are to be received from or transferred to someone other than a person that has been verified as a customer or beneficial owner, the reasons behind the payment/transfer and the capacity of the third party will need to be understood, and consideration given to the extent to which their identity may need to be verified. Whether this is the responsibility of the firm itself, or a separate custodian, will depend on how custody is provided and the firm's role with regard to the payment or transfer. The different likely scenarios are discussed in the following paragraphs.

Note that this issue concerns additions to and withdrawals from the customer's portfolio, as opposed to the settlement of transactions undertaken by the firm in the course of managing the portfolio.

- 9.25 Where the customer enters into an agreement directly with a custodian other than the firm, it is the custodian that should be concerned about third party payments and transfers. The firm should consider the issue itself, however, where it is involved in

FINAL BOARD APPROVED

the transmission of funds or otherwise passes instructions to the custodian regarding a receipt or withdrawal of funds/investments.

- 9.26 The firm may provide custody notionally as part of its service to the customer, but outsource the safe-keeping function to a sub-custodian. In these circumstances, the firm will usually instruct the sub-custodian regarding receipts or withdrawals from the portfolio and should therefore take appropriate steps to verify the identity of any third party that may be involved. The firm should also ensure that the issue is addressed, either by itself or by the sub-custodian, where the customer is able to instruct the sub-custodian directly.
- 9.27 The firm may perform the custody function in-house, in which case it must take appropriate steps itself to verify the identity any third parties that may be involved.
- 9.28 In any event, where the firm is asked to receive, make or arrange payment to/from someone other than a person it has verified as a customer or beneficial owner, it should seek to understand the reasons behind the payment and the capacity of the third party and consider the extent to which the identity of that third party may need to be verified.

Timing

- 9.29 Firms must verify a customer's identity as soon as practicable after first contact with the customer. While most institutional customers will be identified before funding their account, they are not prevented from entering into the relationship. Firms should take all reasonable steps to verify the customer's identity within a reasonable time. Where the firm is unable to verify the identity of the investor within a reasonable time it must, at that point, consider if the circumstances give any grounds to suspect money laundering or terrorist financing and act accordingly (see Part I, paragraph 5.2.8).
- 9.30 If, however, after such reasonable time, the firm has no grounds to suspect and is satisfied that the risk of money laundering is minimal, subject to its terms of business it must terminate the relationship and return any monies received to their source. Alternatively, if the firm is suspicious, it must submit a SAR to the NCA. If it does not receive consent to money laundering to return the money, the firm must freeze any funds or assets pending eventual verification (see Part I, paragraph 5.2.9).
- 9.31 From the point at which the firm concludes it should *freeze* an investment:
- (a) it must not accept further investments from the customer until they provide the evidence of identity required by the firm;
 - (b) it may permit the investor to withdraw their investment upon production of the evidence of identity required by the firm;
 - (d) it should otherwise continue to act in accordance with any relevant terms of business and regulatory obligations until such time as the relationship may be terminated (this would include issuing periodic statements and managing the customer's portfolio where this does not involve the investment or withdrawal of capital); and

FINAL BOARD APPROVED

(e) it must take steps to remind customers (individually or generically, as appropriate according to their risk-based approach) that evidence of identity may still be required, noting the consequences of failure to comply with the firm's request.

- 9.32 Firms are recommended to include in their terms of business that they may return or freeze the customer's investments unless or until the necessary evidence of identity can be obtained.

Additional customer information

- 9.33 The client take-on process for investment management customers usually involves gaining an understanding of the customer, including their source of wealth and income, and their needs, and establishing at the outset the likely inflows and outflows of funds are likely. Developments in this area and updates to customer information should be sought periodically from the customer or his adviser.
- 9.34 The customer information, obtained for the purposes of agreeing the firm's mandate and the ongoing management of the customer's portfolio, will usually comprise the additional information necessary to understand the nature and purpose of the relationship in a money laundering context, against which the customer's future activity should be considered.

Monitoring

- 9.35 Customer activity relates only to inflows and outflows of money that do not relate to the firm's own dealings in the portfolio of investments. Most movements into or out of the portfolio will usually be expected (e.g. pension scheme contributions or funding of pensions benefits). The firm should establish the rationale behind any unexpected ad hoc payments made or requested by the customer.

Non-liquid transactions (including Real estate)

- 9.36 Some portfolios will include direct holdings in real estate. Unlike securities, the counterparties involved in the purchase and sale of direct holdings may not be other regulated financial institutions. Those purchases and sales will often involve special purpose vehicles, and in some cases will be owned via trusts and a wide variety of structures in a wide variety of jurisdictions which by their nature may increase the risk of coming into contact with the proceeds of crime.
- 9.37 Some portfolios will make direct investments in construction and development projects. The nature of these projects, and especially the risks of fraud, bribery and corruption and tax evasion may also increase the likelihood of coming into contact with the proceeds of crime.
- 9.38 The counterparty would not normally be regarded as a customer of the investment firm and consequently the firm would not be obliged to verify the identity of the counterparty itself. However, in order to mitigate what could be significant reputational risk, firms may wish to seek appropriate assurances from their own solicitors that the identity of the counterparty will have been verified.

FINAL BOARD APPROVED

- 9.39 These transactions are generally conducted through solicitors, and the counterparty's solicitor may agree to verify its customer's identity. However, where they do not consent, firms must consider what level of information they require, this could, for instance, be in line with the firm's risk based approach and with Chapter 5 of Part I.

10: Execution-only stockbrokers

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 10.1 *Execution-only (ExO) stockbrokers* carry out transactions in securities with regulated market counterparties, as agent for individual customers. ExO transactions are carried out only on the instructions of the customer.
- 10.2 The guidance contained in this section covers only the purchase and sale of securities, investments (including investment funds), [gilts, warrants and associated cash management services](#). Firms that arrange for customers to invest through third party products or services (e.g., ISAs, fund supermarkets) may be asked to provide confirmation of the customer due diligence they have undertaken to the provider of that product/service (sector 8: *Non-life providers of investment fund products*). See sector 9: *Discretionary and advisory investment management*.

What are the money laundering risks relating to execution-only stockbroking?

- 10.3 Some ExO stockbrokers deal with high volumes of low value customer transactions, whereas others direct their services towards higher net worth customers, and thus have fewer customers. Stockbroking customers may adopt a variety of trading patterns; the firm is offering no advice and may have little or no knowledge of a particular customer's motives.
- 10.4 ExO customers are also free to spread their activities across a variety of brokers in different jurisdictions for perfectly valid reasons, and often do. Each broker may therefore actually have little in terms of transaction history from which to identify unusual behaviour. Many firms provide ExO stockbroking services on a non-face-to-face basis, including via the internet.
- 10.5 In view of the above, whilst stockbroking might be regarded as being of lower risk compared to many financial products and services, the risk is not as low as in providing investment management services to the same types of customer from similar jurisdictions.

Who is the customer for AML purposes?

- 10.6 The typical customers for ExO retail stockbroking are individuals. However, customers also include solicitors, accountants and financial advisers, as well as trusts, companies, charities, etc. Much ExO business can comprise occasional, or linked, transactions of a value less than €15,000, which therefore fall within the exemption in Part I, paragraph 5.3.6.

Customer Due Diligence

Verification of identity

- 10.7 There is nothing about typical ExO business in particular that requires the firm to carry out enhanced identity checks as a result of the service offered. Verification of identity for particular types of customer should therefore be performed in accordance with the standard set out in Part I, section 5.3.

FINAL BOARD APPROVED

- 10.8 The risk level of execution only broking, however, depends on whether the services are offered and operated on a face-to-face or non face-to-face basis. The ML Regulations identify non-face-to-face business as a higher risk for money laundering than face-to-face business. In view of this, firms need to have in place additional measures to neutralise the higher risk when opening and operating accounts for non face-to-face business. This can take the form of additional due diligence at the point of account opening, appropriate ongoing monitoring of customer activity or both.

Timing

- 10.9 Verification of identity should be carried out as part of establishing the relationship, but before any services are provided. In the case of share transactions where this might interrupt the normal course of business, verification of identity should take place as soon as practicable after the transaction and in any event before final settlement with the customer. Further details on timing can be found in Part I, paragraphs 5.2.1 to 5.2.5.

Additional customer information

- 10.10 ExO business is driven by the customer and, as mentioned earlier, customer behaviour may vary widely, from the occasional transaction in a FTSE 100 share to day trading in a variety of instruments and markets. Given the reasonably narrow range of services provided by ExO stockbrokers, no additional information is likely to be required to establish the purpose and intended nature of the business relationship.

Monitoring

- 10.11 As mentioned above, customer behaviour may vary widely, therefore making it harder to pick up unusual or suspicious trading activity. Attention should, therefore, be focused on ensuring that payments to and from the customer as a result of trading activity are conducted through a bank or building society account in the UK, the EU or in an assessed low risk jurisdiction.
- 10.12 Where a firm is transacting business for a customer who has opened and operated an account on a non face-to-face basis, and the payment is proposed to be made into an overseas account, then the firm should mitigate the higher risk of the non face-to-face business by establishing that the overseas account is held in the customer's own name. If the firm is not able to establish that the account is held in the customer's own name, it should proceed with caution. The firm should consider review of the account and transaction history, and the reason for making the payment abroad, to determine whether the account, or any dealings on the account, are unusual, and therefore possibly suspicious. If the firm has doubts about the proposed transaction, then an external disclosure to the NCA should be made, and appropriate consent obtained, prior to making the overseas payment.
- 10.13 Where a firm's product range allows a customer to make third party deposits or payments, for example through linked banking services, the firm must assess the higher risk presented by these transaction types and enhance its monitoring and staff training accordingly to mitigate.

11. Motor finance

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance, and the guidance in sector 12: Asset finance.

Overview of the sector

- 11.1 Motor finance companies offer a number of products to fund the acquisition and use of a motor vehicle. Dependent upon the funding method used, the customer may or may not obtain legal title to the vehicle. Motor finance products generally fall into two categories – purchase agreements, and lease agreements.

Purchase agreements

- 11.2 *Conditional sale* is a contract between the finance company and the customer where the customer agrees to buy specific goods. It is normally a fixed cost, fixed term credit and the customer in practice exercises all the rights of the owner of the goods. However, in law, the ownership of the asset will not pass until certain conditions are met (normally that all payments under the contract have been made, but individual contracts may include other conditions).
- 11.3 *Hire Purchase (HP)* and *Lease Purchase (LP)*. These are both agreements under which the customer will hire the vehicle for a fixed period of time. During this period the motor finance company will recover, through the instalments paid, the cost of the vehicle together with its charges. Once the agreement is paid in full, the customer has the option to purchase the vehicle for a nominal sum. Generally, the difference between the two agreements is that on HP the amount to be repaid is spread evenly throughout the agreement, whereas on LP a substantial sum is deferred to the final instalment.
- 11.4 *Personal Contract Purchase (PCP)* is in essence a purchase agreement (the definition would, therefore, be the same as HP and LP) with a Guaranteed Minimum Future Value (GMFV) placed on the goods by the finance company. The customer has the choice at the end of the agreement of either paying the GMFV and obtaining title to the vehicle or returning the vehicle (and not having to pay the GMFV).
- 11.5 *Personal Loan* is an agreement where the title passes immediately to the customer and an unsecured loan is provided to cover all or a proportion of the sale price.

Lease agreements

- 11.6 These are agreements where the customer leases the vehicle for a fixed period of time, but does not have the ability to obtain title. The motor finance company will reclaim the VAT on the vehicle and claim writing down allowances for tax purposes, as owner of the asset. A business customer can, dependent upon its tax position, claim both tax relief and proportion of the VAT on rentals paid. There are two types of lease:
- A *Finance Lease*, where the customer takes the risk in the final value of the vehicle.
 - An *Operating Lease*, where the motor finance company takes the risks and rewards in the final value of the vehicle. Where the customer is a private individual the finance product is known as *Personal Contract Hire (PCH)*

FINAL BOARD APPROVED

- 11.7 This guidance applies to all dealer-introduced motor finance, unless otherwise stated (as in the case for operating leasing (see 11.8 below)) including, but not limited to, cars, light commercial vehicles, motorcycles and caravans. However, brokers are not covered by the money laundering regulations unless they provide finance leasing products on their own books.
- 11.8 Operating leases¹⁴ are **outside** the scope of the ML Regulations¹⁵. However, in practice for some firms it may be difficult to separate out this type of activity from other forms of leases, such as finance leases. In these circumstances ‘best practice’ would suggest that firms *may* nevertheless wish to make a commercial decision to follow this guidance in respect of this type of lease.

What are the money laundering risks in motor finance?

- 11.9 The features of all lending are generally that the initial monies advanced are paid into another bank account, in the case of motor finance in exchange for the use of a vehicle. Repayments are usually made from other bank or building society accounts by direct debit; in most, but not all, cases, repayments in cash are not, and should not be, encouraged.
- 11.10 Given that a loan results in the borrower not receiving funds from the lender, but the use of a vehicle, the initial transaction is not very susceptible to money laundering. The main money laundering risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination. Early repayment can also be indicative of funds being used which have emanated from a criminal lifestyle.
- 11.11 Motor finance products therefore carry a low inherent money laundering risk. A motor finance company will normally only accept payment of instalments from the customer named on the agreement, and in the case of overpayment will only make repayment to the customer named on the agreement.
- 11.12 Should a motor finance company accept occasional payments from third parties, for example the settlement of the agreement by the dealer, and/or accept payment via payment books, it must be alert to the increased risk of receiving the proceeds of crime.

Assessment of the risk

- 11.13 The lender’s knowledge of the customer only extends to information gleaned at the identification stage, and to a single monthly payment on the agreement; their occupation details and monthly income/expenditure are generally unknown.
- 11.14 The nature of motor finance business, however, is that the type of agreement entered into with the customer carries a low risk of money laundering.
- 11.15 Procedures and controls used for identifying potential money laundering are therefore normally transactional-based, to identify unusual transactional movements, unusual deposits, unusual advance payments or unusual repayment patterns.

¹⁴ Vehicle contract hire and vehicle rental products would, for the purpose of this guide and accounting purposes, be classified as being an operating lease and as such would fall **outside** the scope of this guide. Under Financial Reporting Standard 5 (“FRS5”) and Statement of Standard Accounting Practice 21 (“SSAP 21”) operating leases would be a lease where risk and rewards of ownership do not pass substantially to the lessee.

¹⁵ Whilst Operating leases fall outside the requirements of the Money Laundering Regulations, firms should be aware of the anti-money laundering reporting requirements of the Proceeds of Crime 2002 (POCA), which covers all types of business. See, for example, paragraphs 1.36-1.37 in Part I of the Guidance.

FINAL BOARD APPROVED***Who is the customer for AML purposes?***

- 11.16 A customer may be a private individual or a business e.g., partnerships, companies, associations etc.
- 11.17 Customers may be introduced through dealers, brokers or by direct lending over the internet, through the post, or by telephone. Motor dealers introduce their customers to lenders whenever finance is required to support a vehicle acquisition. The dealer/lender relationship will be formalised in terms of an agency contract, and the dealer staff conducts face-to-face negotiations. Motor products may also be obtained remotely either directly through a lender application or website or indirectly through a broker application or website, without face-to-face contact; this is likely to carry a higher risk.

Customer due diligence

- 11.18 In a move to reduce fraudulent credit applications, members of the Finance & Leasing Association (FLA) have subscribed to an industry standard which sets out acceptable identification and verification checks across common sales channels for obtaining motor finance. The Industry Standard is set out in the attached Annex 11-I.
- 11.19 Compliance with the Industry Standard on proof of identity goes beyond the current money laundering requirements under simplified due diligence (SDD), which is directly relevant for low risk products such as hire purchase and leasing agreements. However, this Industry Standard should still be used in order to guard against fraud. On-going monitoring of the business relationship is still required under simplified due diligence (SDD).



FLA INDUSTRY STANDARD FOR THE PREVENTION OF FINANCIAL CRIME AND TERRORIST FINANCING IN MOTOR FINANCE CREDIT APPLICATION PROCESSING

INTRODUCTION

1. Finance and Leasing Association (FLA) motor finance members have both a legal and moral obligation to ensure that they correctly identify their customers in the credit application process in order to prevent financial crime and terrorist financing.
2. The requirements set out in the Money Laundering Regulations and the [Joint Money Laundering Steering Group \(JMLSG\) Guidance](#) are the minimum legal requirements that all FLA motor finance members must comply with in the battle against money laundering, fraud and terrorist funding. This document in no way seeks to replace members' legal obligations.
3. The remainder of this Standard sets out the approach required by full FLA members to due diligence when considering a credit application and acceptable methods for conducting these checks. Appendix 1 outlines common sales channels available for obtaining motor finance and identifies for each what evidence of identification (Know Your Customer) and verification of this evidence (Prove Your Customer) is required to meet the Standard.

RISK ASSESSMENT

4. Members will undertake appropriate steps to identify, assess and mitigate the risks of money laundering and terrorist financing to which its business is subject, taking into account information made available by the FCA on risk factors that relate to their customers, products, services, transactions and delivery channels.
5. The assessment of the risks inherent to a member's business will inform its risk-based approach which determines the level of due diligence undertaken for each individual customer. Risk assessments must be documented, kept up to date and made available to the FCA on request.

CUSTOMER DUE DILIGENCE (CDD)

6. There is a fundamental requirement to identify customers and verify their identity through CDD, where they are individuals. Where the customer is a business, members should additionally identify its beneficial owners and be satisfied they know who the owners are. A beneficial owner of a business is a person who owns or controls more than 25% of the business (even indirectly). Where an ongoing business relationship is commenced, there is a requirement to obtain information regarding the purpose of any transactions, and the source of any funds.
7. CDD requirements must be carried out:
 - When establishing a business relationship
 - When carrying out an occasional transaction over €10,000 (or equivalent)
 - Where money laundering or terrorist financing is suspected
 - Where there are doubts about previously obtained customer information
 - As appropriate, for existing customers on a risk-sensitive basis

FINAL BOARD APPROVED

8. The vast majority of transactions completed by FLA motor finance members will usually fall into one of the above categories and therefore fall within the scope of CDD. The level of CDD measures must be taken on a risk sensitive basis, depending on the type of customer, business relationship or product.

SIMPLIFIED DUE DILIGENCE (SDD)

9. Members can apply simplified customer due diligence in relation to a particular business relationship or transaction if it is determined that the business relationship or transaction presents a low degree of risk of money laundering or terrorist financing, taking into account:
- The risk assessment carried out (see paragraph 4 above)
 - Information and guidance from the FCA.
 - Risk factors relating to: the type of customer e.g. business, consumer, financial institution, business listed on a regulated market; where the customer resides or has been established; and the motor finance product and sales channel it is delivered through.

ENHANCED DUE DILIGENCE (EDD)

10. EDD requirements must be carried out on a risk-sensitive basis:
- In any case identified where there is a high risk of money laundering or terrorist financing based on the assessment of risk.
 - In any transaction or business relationship where there is a high risk of money laundering or terrorist financing.
 - When the transaction is with a politically exposed person (PEP) – a person that holds a prominent public function in the UK or overseas – or family member or known close associate of a PEP.
 - Where the transactions are complex, unusually large, follow an unusual pattern or serve no apparent economic or legal purpose.
 - In any other situation which presents a higher risk of money laundering.

EVIDENCE OF IDENTITY

11. As standard under CDD, members must obtain for individuals:
- full name
 - current residential address, and
 - date of birth
12. Members must obtain for business customers:
- full name
 - registered number (if any)
 - registered office in company of incorporation
 - business address
13. Additionally for private or unlisted businesses:
- Names of all directors
 - Names of all beneficial owners (to include ultimate beneficial owner or controlling person)

VERIFICATION OF IDENTITY

14. Members must verify customer identities through reliable and independent sources. This can be done through:

FINAL BOARD APPROVED

- documents provided by the customer, or;
- electronic data, or;
- a combination of both.

For face-to-face identification, originals of any documents should be seen unless electronic identification and verification processes are being used.

15. Members must make checks on the evidence provided to satisfy themselves of the customer's identity, and keep a record of the checks made. Checks include ensuring:

- Visual likeness with the customer and any photo ID
- The customer's date of birth matches the apparent age of the customer
- The ID is valid
- The spelling of names and addresses correspond exactly
- The address on the ID matches the address given

16. Members must be vigilant of forgeries, and should check that the documents are not:

- unclear or fuzzy
- rough or uneven over the required information
- tattered or uneven around any photograph or the required information
- lacking a holographic picture or watermark

17. If any of the above is apparent, members must make further enquiries of the customer, and ask for further evidence of identity.

ELECTRONIC VERIFICATION

18. Electronic verification may be also used to meet a firm's customer identification obligations. However, a firm should first consider whether electronic verification is suitable for its customer base, and should then have regard to the guidance in Part I, paragraphs 5.3.51-5.3.52 and 5.3.79–5.3.84. When using electronically-sourced evidence to verify identity, firms should ensure that they have an adequate understanding of the data sources relied on by the external agencies that supply the evidence. Firms should be satisfied that these sources provide enough cumulative evidence to provide reasonable certainty of a person's identity, and conform with the guidance set out in Part I, Chapter 5. An electronic check that accesses a single database (e.g., Electoral Register check) is normally not enough on its own to verify identity.

NON-FACE-TO-FACE CUSTOMERS

19. Members are obliged to consider non-face-to-face transactions as a customer risk factor that might require the application of EDD, if the transaction or business relationship is deemed to be 'high risk'. In this situation the following steps should be considered :

- Seeking additional independent, reliable sources or information to verify the customer's identity
- Taking supplementary measures to verify and certify the documents supplied
- Ensuring that the first payment will be carried out through an account opened in the customer's name with a credit institution
- Communicating with the customer at a verified address
- Maintaining ongoing monitoring of the customer's transactions
- Providing an Internet sign-on password to a verified address

FINAL BOARD APPROVED

RELYING ON ANOTHER PARTY TO COMPLETE CDD/EDD MEASURES

20. Members may rely on a third party (e.g. a supplying dealer or online broker) to carry out CDD and EDD measures (for which members are ultimately responsible). However, members must take steps to ensure that the third party will (if requested):

- As soon as possible make available to it any information about the customer (and any beneficial owner) which the third party obtained when applying CDD/EDD measures.
- As soon as possible send it certified copies of standard proofs, 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.
- If the member relies on a 3rd party to complete checks, responsibility for completion of adequate CDD checks remains with the member and appropriate quality assurance procedures should be put in place.

21. Finally, members should be aware of the requirements for senior management responsibility, ongoing monitoring of customers, staff awareness and training, and record keeping requirements which are not subject to this Standard.

BEST PRACTICE: GOING BEYOND THE FLA STANDARD

22. FLA members have identified several other processes that lenders might wish to consider to further strengthen their resilience to fraud, these are:

23. Private customers

- **Obtaining an insurance certificate** from the customer to satisfy that the person insured to drive the vehicle is the same person listed on the finance agreement (and therefore no fronting has taken place). An insurance certificate would also reveal the level of excess the customer is subject to if they need to make a claim. Lenders can assess whether this falls within the terms and conditions of the agreement and that the level of excess is affordable.
- **Asking the customer to share their driving licence details** using the DVLA's Share Driving Licence service. This information will provide lenders with details which used to be provided on the paper counterpart. The service confirms that the driver has not been disqualified or has any medical conditions which prevent them from driving, or limitations to the vehicles they can drive. The customer would need to know their driver number, NI number and post code in order to share their driver record. The DVLA's premium line service can also provide this information.
- **Investigating the source of funds for any large deposits**, particularly those made above €10,000 and/or where such a deposit is out of keeping with the customer's known financial status.
- **Request self-employed trading accounts, SA302 and corresponding tax year overview or bank statements** if the customer does not hold a permanent job and an affordability check returns indifferent results.
- **Verification of the customer on delivery of the vehicle** should be considered for non-face-to-face transactions. The vehicle could be delivered to a verifiable address associated with the

FINAL BOARD APPROVED

contract holder. It could then be handed over to the individual making/signing the agreement who can produce picture ID that appears valid and contains details that are consistent with previously supplied information.

24. Business customers

- **Identify and verify all beneficial owners (including ultimate beneficial owner)** by carrying out the same CDD checks that would be made for private customers/individuals and screening them against PEPs and sanctions lists.
- **Identify and verify all directors or key directors** (including Finance Director and Managing Director) by carrying out the same CDD checks that would be made for private customers/individuals and screening them against PEPs and sanctions lists.

Members might wish to apply the above checks where the business is deemed a higher risk.

25. Supplier due diligence

- **Validating the supplier** to ensure the broker or dealer referring the customer is a legitimate business. Checks include:
 - Ensuring the business is FCA authorised or has interim permission by checking the [Financial Services](#) register.
 - Checking the website and company details.
 - Checking the address using web tools such as Google maps to confirm the external building looks like a valid business.
 - Contacting a business situated nearby to ask if the supplier are an active company.
 - Checking previous accounts information on Companies House (if not a new business) or those available from a Credit Reference Agency for corporate information.

Appendix 1

ACCEPTABLE EVIDENCE OF IDENTITY

Listed below are common sales channels for obtaining motor finance along with the corresponding identification and verification practices deemed acceptable under the Standard.

The Standard is not designed to stop any individual lender adopting a risk based approach within what is/is not acceptable for each sub division of the JMLSG guidance, e.g. any pass rate for Knowledge Based Authentication questions. It instead attempts to deliver a standard industry wide approach to ensure the FLA membership is legally compliant and implements effective risk based anti-fraud measures.

Category 1
Face-to-Face Transaction

Definition

Where the customer has a '**direct and face to face**' interaction with the finance company or a recognised, known and appointed agent of the finance company.

Note: Even if the member relies on a 3rd party to complete checks, responsibility for completion of adequate CDD checks remains with the finance provider.

Examples

- Manufacturer captive or independent finance company providing finance to an individual at an FCA registered and franchised Dealership.
- Direct approach from a customer into a 'branch' of the finance company.

Identification Options

Photo Identification
Know Your Customer / Prove Your Customer
➤ Passport
➤ Photo Card Driving Licence
➤ National Identity Card
➤ HM Forces ID card
➤ Firearms certificate or shotgun licence
➤ Identity card issued by the Electoral Office for Northern Ireland
<i>Any of the above documents can be used on their own for Category 1 customers</i>

Or

Non Photo Identification	
Section 1	Section 2

FINAL BOARD APPROVED

Know Your Customer	Prove Your Customer
<ul style="list-style-type: none"> ➤ 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 	<ul style="list-style-type: none"> ➤ Instrument of a court appointment ➤ Current council tax demand letter, or statement ➤ Current bank statement, or credit/debit card statement, issued by a regulated financial sector firm in the UK, EU or an assessed low risk jurisdiction ➤ Utility bills issued by a UK regulated electric, gas, water or telephone/mobile telephone provider
<p><i>One document from Section 1 and one from section 2 is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below). Bank statements, council tax letters and bills must be current (date must be within the last 3 months)</i></p>	

The original of any physical document must be in date, seen and endorsed by the Finance Company or their recognised, known and appointed agent as “A Fair and true likeness of the individual and a True Copy of the original” in the case of any photographic Identification. Alternatively “A True Copy of the original” in the case of non-photo I.D. documents.

Or

Electronic Identification via an approved supplying agency	
Section 1	Section 2
Know Your Customer	Prove Your Customer
<ul style="list-style-type: none"> ➤ One match on an individual’s full name and current address <p>and</p> <ul style="list-style-type: none"> ➤ A match on the individual’s full name and either his current address or his date of birth. <p>Examples of potential likely data matches are:</p> <ul style="list-style-type: none"> ○ Voters roll ○ Public data e.g. CCJ ○ Digital account information 	<ul style="list-style-type: none"> ➤ Confirming the first payment to be carried out through an account confirmed in the customer’s name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction ➤ Knowledge Based Authentication questions ➤ Verify Debit/Credit Card in customers name and not stolen ➤ Send confirming letters to the customer’s verified address with either return information required, or passwords, internet log-ins etc. ➤ Any other credible and proven verification test that detects impersonation.
<p><i>The two sections need completing separately in order to comply</i></p>	

Or a combination of any of the above sections 1 and 2 to ensure that there is at least one ‘Know Your Customer’ and one ‘Prove Your Customer’.

Category 2

FINAL BOARD APPROVED

Non-Face-to-Face Transactions with the Finance Company, but Face to Face customer contact with an FCA authorised motor dealer**Definition**

Where the customer has a '**direct and face to face**' interaction with an FCA authorised dealer, but the finance company has no direct contact with the customer, nor is part of the same group as the dealer.

Note: Even if the member relies on a 3rd party to complete checks, responsibility for completion of adequate CDD checks remains with the finance provider.

Examples

- Customer attending a non-franchised, independent FCA authorised dealer and being introduced to an independent Finance company direct by the dealer or via a broker.

Identification**Options**

Documentation	
Section 1	Section 2
Know Your Customer	Prove Your Customer
<ul style="list-style-type: none"> ➤ Passport ➤ Photocard Driving Licence ➤ National Identity Card ➤ HM Forces ID card ➤ Firearms certificate or shotgun licence ➤ Identity card issued by the Electoral Office for Northern Ireland ➤ 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 	<ul style="list-style-type: none"> ➤ Instrument of a court appointment ➤ Current council tax demand letter, or statement ➤ Current bank statement, or credit/debit card statement, issued by a regulated financial sector firm in the UK, EU or an assessed low risk jurisdiction ➤ Utility bills issued by a UK regulated electric, gas, water or telephone/mobile telephone provider
<p><i>One document from each section above is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below). Bank statements, council tax letters and bills must be current (date must be within the last 3 months)</i></p>	

The original of any physical document must be in date, seen and endorsed by the Finance Company or their recognised, known and appointed agent as "A Fair and true likeness of the individual and a True Copy of the original" in the case of any photographic Identification. Alternatively "A True Copy of the original" in the case of non-photo I.D. documents.

Or

Electronic Identification via an approved supplying agency	
Section 1	Section 2
Know Your Customer	Prove Your Customer

FINAL BOARD APPROVED

<ul style="list-style-type: none"> ➤ One match on an individual's full name and current address and ➤ A match on the individual's full name and either his current address or his date of birth. <p>Examples of potential likely data matches are:</p> <ul style="list-style-type: none"> ○ Voters roll ○ Public data e.g. CCJ ○ Digital account information 	<ul style="list-style-type: none"> ➤ Confirming the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction ➤ Knowledge Based Authentication questions ➤ Verify Debit/Credit Card in customer's name and not stolen ➤ Send confirming letters to the customers verified address with either return information required, or passwords, internet log-ins etc.
<p><i>The two sections need completing separately in order to comply</i></p>	

Or

Electronic Identification and Documentation	
Section 1	Section 2
Know Your Customer	Prove Your Customer
<ul style="list-style-type: none"> ➤ One match on an individual's full name and current address and ➤ A match on the individual's full name and either his current address or his date of birth. <p>Examples of potential likely data matches are:</p> <ul style="list-style-type: none"> ○ Voters roll ○ Public data e.g. CCJ Digital account information 	<ul style="list-style-type: none"> ➤ Passport ➤ Photocard Driving Licence ➤ National Identity Card ➤ HM Forces ID card ➤ Firearms certificate or shotgun licence ➤ Identity card issued by the Electoral Office for Northern Ireland ➤ Valid (old style) full UK driving licence <p>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</p>
<p><i>One document from each section above is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below).</i></p>	

The original of any physical document must be in date, seen and endorsed by the Finance Company or their recognised, known and appointed agent as "A Fair and true likeness of the individual and a True Copy of the original" in the case of any photographic Identification. Alternatively "A True Copy of the original" in the case of non-photo I.D. documents.

Or

a combination of section 1 and section 2 checks from any of the three tables, ensuring you are satisfied of a risk based approach that is delivering both 'Know Your Customer' and 'Prove Your Customer'

Category 3

FINAL BOARD APPROVED

Non-Face-to-Face Transactions, where the finance company, dealer or broker has had no face to face contact with the customer**Definition**

Where the customer has applied direct to the finance company, dealer or broker (potentially via the internet) and it is unlikely a suitably authorised individual will see the customer face to face to take and verify any ID documents.

Note: Even if the member relies on a 3rd party to complete checks, responsibility for completion of adequate CDD checks remains with the finance provider.

Examples

- Internet application to an 'online broker' who sources a vehicle for the applicant, introduces the customer direct to a finance company and delivers the car to the customer, self-invoicing the deal to the finance company.
- Direct application to a finance company who then place the customer into a dealership.

Identification Options

Electronic Identification via an approved supplying agency	
Section 1	Section 2
Know Your Customer	Prove Your Customer
<p>➤ One match on an individual's full name and current address and</p> <p>➤ A match on the individual's full name and either his current address or his date of birth.</p> <p>Examples of potential likely data matches are:</p> <ul style="list-style-type: none"> ○ Voters roll ○ Public data e.g. CCJ ○ Digital account information 	<p>➤ Confirming the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction</p> <p>➤ Knowledge Based Authentication questions</p> <p>➤ Verify Debit/Credit Card in customer's name and not stolen</p> <p>➤ Send confirming letters to the customer's verified address with either return information required, or passwords, internet log-ins etc.</p> <p>➤ Any other credible and proven verification test that detects impersonation.</p>
<p><i>The two sections need completing separately in order to comply. Information from section 1 can include details provided through any form of correspondence with the customer or a third party</i></p>	

Additional verification check

FINAL BOARD APPROVED

Where identity is verified electronically, copy documents are used or where the customer is not physically present members should apply an additional verification check to manage the risk of impersonation fraud. Acceptable methods of check include:

- Verifying with the customer additional aspects of their identity (biometric data) which are held electronically;
- Requesting the applicant to confirm a secret PIN or biometric factor that links them incontrovertibly to the claimed identity.
- An additional verification check consisting of robust anti-fraud checks that members routinely undertake as part of their existing procedures (see Section 2 above).

11A: Consumer credit providers

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the Sector

- 11A.1 Firms that undertake consumer credit businesses (but are not regulated for non-credit activities by the FCA before 1 April 2014) are subject to the provisions of the Money Laundering Regulations 2017, as they provide lending within point 2 of Schedule 2 of the ML Regulations. Some professional firms that provide consumer credit services and are subject to a designated professional body will not be required to be authorized, as they can take advantage of the FCA PROF Handbook, which means their compliance is overseen by their professional body.
- 11A.2 Certain consumer credit businesses (such as some pawnbrokers) which also undertake money service business activity, although authorised by the FCA for their consumer credit activity, will continue to be subject to supervision by HMRC¹⁶. These businesses should follow HMRC guidance for the MSB sector¹⁷ but may find this guidance useful for their consumer credit activity.
- 11A.3 Consumer credit providers are therefore subject to the full provisions of UK law and regulation relating to the prevention of money laundering and terrorist financing. The guidance in Part I therefore applies to all consumer credit providers. Consumer credit providers are also subject to the FCA financial crime rules in SYSC 6.1.1 and 6.3.

Typical products

- 11A.4 Consumer credit providers covered by this guidance include both unsecured credit providers and secured lenders. Products provided include:
- Store cards and other revolving credit facilities¹⁸
 - Point of sale or other retail finance
 - Personal loans or short term credit
 - Second charge lending¹⁹
 - Secured loan provided by a pawnbroker
- 11A.5 The amounts lent are generally but not always under £25,000 and for periods of between 2-5 years (although some lenders provide larger value finance over longer terms for home improvements or for secured loans and substantially shorter for short-term, low value loans or interest free finance)²⁰. This guidance will also be relevant to those businesses who sell goods or services on credit (although hire purchase is addressed in Sector 11: *Motor Finance*).

¹⁶ This applies where a consumer credit business falls within the definition of an “excluded money service business” in Regulation 7(5).

¹⁷ www.hmrc.gov.uk/mlr

¹⁸ Credit Card Issuers are, however, covered by separate guidance in Part II, Sector 2: *Credit cards*

¹⁹ But not first charge lending

²⁰ There are no time constraints on revolving credit.

FINAL BOARD APPROVED

What are the money laundering or terrorist financing risks for consumer credit providers?

- 11A.6 With the exception of store cards or revolving credit facilities, the features of the lending are generally that the initial monies advanced are paid into the customer's own or another bank account, e.g. the Point of Sale retailer. Repayments are usually made from the customer's own bank or building society accounts by direct debit. Repayments in cash are not, and should not be, encouraged.
- 11A.7 Generally, consumer credit providers do not hold permission from the FCA to handle client money (although other parts of the businesses may do if they are part of larger retail banking groups), so in practice there is unlikely to be any involvement in the placement stage of money laundering. There is, however, scope for consumer credit providers to be drawn in to the layering and integration stages.
- 11A.8 The main money laundering risks arise through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination or settlement. Consumer credit providers should be aware that early repayments carry a risk that the funds have emanated from a criminal lifestyle.
- 11A.9 Overall, however, the provision of consumer credit carries a low inherent money laundering/terrorist financing risk. Lenders will normally only accept payment of instalments from the customer named on the agreement, and in the case of an overpayment will only make repayment to the customer named on the agreement.
- 11A.10 However, if a consumer credit provider accepts occasional payments from third parties, for example, on settlement of the agreement, it must be alert to the unknown nature of the source of these funds, which may increase the risk of receiving the proceeds of crime. There is also a risk for pawnbrokers providing a secured loan, that the goods held as security may be the proceeds of crime.

Assessment of the risk

- 11A.11 For single advance finance, the lender's knowledge of the customer (other than an existing customer) only extends to information gleaned at the identification stage, and to a single monthly payment²¹ on the agreement. Their occupation details and income are generally known and the applicant's details are usually validated by searches at one or more of the Credit Reference Agencies.
- 11A.12 For Store cards and revolving credit facilities, additional reviews are undertaken on a regular basis to update the customer details.
- 11A.13 The nature of consumer credit, however, is that the type of agreement entered into with the customer carries a relatively low risk of money laundering.
- 11A.14 Consumer credit can be provided through a number of different channels. Customers may be introduced through the internet, via the telephone, by post or face to face. Where lending is obtained remotely without face-to-face contact, this is likely to carry a higher risk.
- 11A.15 Procedures and controls used for identifying potential money laundering are therefore normally transactional-based, to identify unusual transactional movements, unusual deposits, unusual advance payments or unusual repayment patterns.

Customer Due Diligence (CDD)

- 11A.16 Having sufficient information about customers and beneficial owners and using that

²¹ This may slightly vary by form of credit.

FINAL BOARD APPROVED

information underpins all other anti-money laundering procedures. A firm must not enter into a business relationship until the identity of all the relevant parties to the relationship has been verified in accordance with the guidance in Part I, Chapter 5.

- 11A.17 The borrower in respect of consumer credit tends to be a private individual, although loans of these types can be made for business purposes to sole traders and partnerships of two or three partners (not all of whom are corporate entities). If the borrower is a large partnership, a limited liability partnership or a private or public company, the borrowing will not be regulated by the Consumer Credit Act 1974 but the business must obtain information that is relevant to that entity such as company registration number and registered address. For all business entities, it is prudent to obtain (where relevant) evidence that individuals have the authority to act for that entity and evidence to establish beneficial owners of such entities.
- 11A.18 Further guidance on identification and verification of the customer is given in Part I 5.3.2-5.3.7. Further detail on identification and verification of a beneficial owner is available at 5.3.8-5.3.13. Guidance on the requirements relating to existing customers is set out in Part I at 5.3.14-5.3.17.

Private individuals

- 11A.19 Guidance on verifying the identity of private individual consumers is given in Part I, paragraphs 5.3.57 to 5.3.105. This validation may be undertaken by either the lender or by a broker e.g. for Point of Sale Finance. However, where such a broker is not regulated by the FCA in its own right, it is important to recognize that it may be acting merely as an authorised representative of the lender (see Part I, paragraphs 5.6.34-5.6.43).
- 11A.20 Customers may be assessed as presenting a higher risk of money laundering if they are identified as being Politically Exposed Persons (PEPs), or because of some other aspect of the nature of the customer, or his business, or its location, or because of the product features available. In such cases, the firm must conduct enhanced due diligence measures (see Part I section 5.5) and will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity. For such customers, the lender will need to consider whether to require additional customer information (see Part I, section 5.5) and/or whether to institute enhanced monitoring (see Part I, section 5.7).
- 11A.21 Non face-to-face transactions can present a greater money laundering or terrorist financing risk than those conducted in person because it is inherently more difficult to be sure that the person with whom the firm is dealing is the person that they claim to be. Enhanced due diligence is required in these circumstances, and verification of identity undertaken on a non- face-to-face basis should be carried out in accordance with the guidance given in Part I, paragraphs 5.5.10 to 5.5.17.
- 11A.22 Some persons may not be able to produce the standard evidence of identity. Where customers cannot produce the standard identification of evidence, reference should be made to the guidance set out in sector I: Retail banking, Annex 1-I.

Non Personal Customers

- 11A.23 Guidance on verifying the identity of non-personal customers is given in Part I, paragraphs 5.3.106 to 5.3.168. Categories of non-personal customers that are likely to be of particular relevance to consumer credit providers are:
- small partnerships and unincorporated businesses (paragraphs 5.3.154-5.3.168)
- 11A.24 Consumer credit providers may also want to refer to Part II, Sector 11: *Motor finance*, Annex 11-I sections 1-6. This documents the Industry Standards for Fraud Prevention in Credit

FINAL BOARD APPROVED

Application Processing. This documents standard identification evidence. It should be noted that some of the requirements set out in this industry standard exceed those now required for lower risk products under the current money laundering regulations.

Using verification work carried out by another firm

- 11A.25 The responsibility to be satisfied that a customer's identity has been verified rests with the firm entering into the transaction with the customer. However, where two or more financial transaction, in certain circumstances one firm may use the verification carried out by another firm. Guidance on the circumstances in which such an approach is possible, and on the use of pro-forma confirmation documentation, is given in Part I, section 5.6.
- 11A.26 Consumer credit providers should bear in mind that they are often the party which is carrying out the initial customer identification and verification process.

Suspicious transactions

- 11A.27 Guidance on monitoring customer transactions and activity is set out in Part I, section 5.7. Guidance on internal reporting, reviewing internal reports and making appropriate external reports to the National Crime Agency (NCA), is given in Part I, Chapter 6. This includes guidance on when a firm needs to seek consent to proceed with a suspicious transaction, with which consumer credit providers need to be familiar.

Staff awareness and training

- 11A.28 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions, which may prove to be suspicious.
- 11A.29 Guidance on staff awareness, training and alertness is given in Part I, Chapter 7. This guidance includes suggested questions that staff should be asking themselves, and circumstances that should cause them to ask further questions about particular transactions or customer activity.

Record-keeping

- 11A.30 General guidance on record-keeping is given in Part I, Chapter 8. Verification of the identity of a customer or beneficial owner may be by means of documentation or electronically. Where documents are used, it is preferable to make and retain copies.
- 11A.31 Documents relating to customer identity must be retained for five years from the date the business relationship with the customer has ended (see Part I, paragraph 8.12).

12. Asset Finance

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance and, where relevant, the guidance in sector 11: Motor finance.

Overview of the sector

- 12.1 Asset finance providers offer financial facilities that allow a business to use an asset over a fixed period, in return for regular payments. The business customer chooses the equipment it requires, and the finance company buys it on behalf of the business. There are a number of ways in which a business may finance an asset. These are described below.

Leasing

- 12.2 The fundamental characteristic of a lease is that ownership of the asset never passes to the business customer.
- 12.3 Under a *finance lease*, the leasing company recovers the full cost of the equipment, plus charges, over the period of the lease. It can claim written down allowances, whilst the customer can claim both tax relief and VAT on rentals paid.
- 12.4 An *operating lease* is often used where a business requires a piece of equipment for a shorter period of time, for example construction equipment. The leasing company will lease the equipment to the customer, expecting, at the end of the lease period, to sell it second-hand or to lease it to another customer. The business customer does not enter the operating leased item on its balance sheet as a capital item.
- 12.5 The most common form of operating lease is known as contract hire. Essentially, this gives the customer the use of the asset, together with additional services such as maintenance and repair of the asset. An example of an asset on contract hire would be a fleet of vehicles. In this instance, a proportion of the VAT is reclaimable by the customer.
- 12.6 Operating leases are outside the scope of the ML Regulations²². Best practice would, however, suggest that firms should nevertheless follow this guidance in respect of this type of lease. In any event, in practice it may often be difficult to separate out this type of activity from other forms of lease. For example, many asset finance businesses offer a mixture of operating and finance leases and it would therefore be unduly cumbersome to follow different procedures for different leasing products, as well as inconsistent with a risk based approach.

Purchase

- 12.7 *Hire Purchase* (HP) is a well-established method of financing the purchase of assets by businesses. Under a HP agreement, the customer will hire the asset(s) for a fixed period of time. During this period the asset finance company will recover, through the instalments paid, the cost of the asset(s) together with its charges. Once the agreement is paid in full, the customer has the option to purchase the asset(s) for a nominal sum.

²² Whilst Operating leases fall outside the requirements of the Money Laundering Regulations, firms should be aware of the anti-money laundering reporting requirements of the Proceeds of Crime 2002 (POCA), which covers all types of business. See, for example, paragraphs 1.36-1.37 in Part I of the Guidance.

FINAL BOARD APPROVED

- 12.8 A *lease purchase* is similar to HP, the main difference being in the terms and structure of repayments. Some finance companies differentiate lease purchase from HP by using lease purchase where the customer wishes to defer payment of a substantial part of the asset cost until the end of the agreement.
- 12.9 *Joint ventures* between asset finance providers are commonplace on high value transactions.
- 12.10 The above funding methods are a guide and include variations with or without maintenance e.g., recourse or non-recourse.
- 12.11 *Structured or "big ticket" asset finance* broadly covers very high value transactions. Products are highly visible and high profile, such as aircraft, ships and properties. Here, the lending tends to be higher in quality, generally being made to major reputable companies, be they public sector or at the top end of the private sector. Transactions are one-off and no deposits are generally taken. Most big-ticket financiers are subsidiaries of the major banks; business is often introduced from another part of the group and so information on the customer is contained within a group-wide database.
- 12.12 *Middle market products* include commercial vehicles, cars for business, plant machinery and IT equipment to a wide range of business customers.
- 12.13 At the *"small ticket" end of the market*, products such as photocopiers, PCs and telephone systems depreciate very quickly and offer little incentive for money laundering. Given that the asset provider owns title to the assets, there is little the end user can do with the assets.

What are the money laundering risks in asset finance?

- 12.14 The features of asset finance are generally that no monies are advanced to the customer, but are paid into a supplier's bank account to fund the purchase of an asset which is made available under contract to the customer. Repayments by the customer are usually made from other bank accounts by direct debit; in most, but not all, cases. Repayments in cash are not, and should not be, encouraged. Risk is also associated with hire purchase and lease products as they could be used for layering.
- 12.15 Given that a loan does not result in the borrower receiving funds from the lender, but the use of assets, the initial transaction is not very susceptible of money laundering. The main money laundering risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination. Early repayment can also be indicative of funds being used which have emanated from a criminal lifestyle.
- 12.16 Asset finance products therefore generally carry a low inherent money laundering risk. An asset finance company will normally only accept payment of instalments from the customer named on the agreement, and in the case of overpayment will only make repayment to the customer named on the agreement.
- 12.17 In summary, the business of asset financing can be considered as carrying a low money laundering risk because:
- under a pure leasing agreement, lessees cannot acquire ownership of the asset during the term of the lease;
 - payments are usually collected from other bank accounts by direct debit; and cash payments are not accepted in the normal course of business.

FINAL BOARD APPROVED

Assessment of the risk

- 12.18 In assessing customer risk, reference should be made to the risk-based approaches referred to in Part I, sections 5.4 and 5.5. These sections look at both simplified due diligence (SDD) and enhanced due diligence (EDD).

Customer due diligence

- 12.19 All asset finance providers should carry out full credit searches on the businesses they transact with. Additional steps to verify identity will vary across the three markets, as set out below. Note that this may well go beyond what is required by the current money laundering regulations, certainly in relation to low risk areas which can now rely on simplified due diligence (SDD). However, these additional measures will still be important for fraud purposes.
- 12.20 Under the regulations third parties can be used as agents for customer due diligence purposes in those sectors that are currently subject to established systems of supervision for money laundering. In practice this means that credit and financial institutions authorised and supervised by the FCA for anti-money laundering compliance will be able to be relied upon, although in all cases the 'relying' firm retains ultimate responsibility for meeting the obligations under the Regulations.
- 12.21 *Big-ticket lenders* – Traditionally as part of the credit underwriting process, the lender will check that the lessee is listed on a recognised market or exchange, or is a subsidiary of such a company. The lender should also check whether the lessee is a local authority. Where the customer is not listed, the standard verification requirement set out in Part I, paragraphs 5.3.140 – 5.3.145 is usually followed, including appropriate verification of the identity of the beneficial owners. Where appropriate, verification of the identity of the directors in principal control, and company searches, will be undertaken as part of normal underwriting procedures.
- 12.22 Prior to agreeing to finance an asset, the lessor will sometimes visit the lessee. There should be an understanding of the client's business; for example, that the nature of the asset for which funding is sought is consistent with the business.
- 12.23 *Middle market asset financiers* also follow the procedures set out in Part I, section 5.3, making full use of data held by credit reference agencies. This will verify key parties/directors, including beneficial owners. As with providers of structured asset finance, prior to agreeing to finance an asset, the lessor will usually visit the lessee and have an understanding of the client's business. However, in applying a risk-based approach, middle market asset financiers may take appropriate account of the guidance on using the source of funds as evidence of identity given in Part I, paragraphs 5.3.82- 5.3.87. There will be variations, depending on whether a company is listed on a regulated market or exchange, and other exceptions which may be relevant as set out in Part I, Chapter 5.
- 12.24 *Small ticket lenders* may be able to rely on simplified due diligence (SDD) as set out in Part I, section 5.4 and are, therefore, no longer required to verify identity in accordance with the standard requirements set out in Part I, paragraphs 5.3.106 - 5.3.272. This is because this is a particularly low risk area. However, for fraud purposes lenders should still carry out identity verification in accordance with standard practice.
- 12.25 There may be variations, depending on whether a company is listed on a regulated market or exchange, and other exceptions which may be relevant as set out in Part I, Chapter 5.
- 12.26 Where identity is still required for a transaction which may be seen as higher risk the Asset finance business would be able to use the source of funds as evidence of identity (see Part I,

FINAL BOARD APPROVED

paragraphs 5.3.82 – 5.3.87), provided that repayment is to be made by direct debit from an account that can be confirmed at the outset as being in the borrower's name. However, where the sum being lent is to be paid direct to the customer's supplier, sufficient due diligence must be carried out to ensure that the supplier is genuine.

- 12.27 For sole traders or small partnerships, the standard identification requirement set out in Part 1, paragraphs 5.3.154 - 5.3.163 should be followed. Where the risks are considered at their lowest, firms may be able to carry out simplified due diligence as set out in Part I, section 5.4.

OUTDATED VERSION

13: Private Equity

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 13.1 Private equity firms in the UK are subject to the ML Regulations as they are generally “financial institutions” within the meaning of the ML Regulations.
- 13.2 For the purposes of this guidance, private equity means a form of equity investment into companies and encompasses areas of fundraising and transactional activity:
- **Fundraising:** Marketing and raising private equity funds. Capital is raised from a variety of investors (see paragraph 13.9) who can commit large sums of money for long periods of time.
 - **Transactions:** Entering into private equity transactions. This involves:
 - Investing the capital raised in private equity funds and/or proprietary capital, by providing long term finance to a range of businesses, from early stage companies to large established corporate groups. Capital is usually invested in private companies but may be used to buy out (take private) public companies whose equity is subsequently delisted;
 - Syndicating equity to co-investors;
 - Managing portfolios of investments (often involving participation on company boards as non-executive directors) and exercising negotiated shareholder rights;
 - Acquiring or selling debt instruments or derivatives;
 - Transactions by a portfolio company which will result in a realisation or return for, or a further investment being provided by, a private equity fund; and
 - Realising the investment by way of a full or partial private sale or an IPO of the portfolio company.

The rest of this sectoral guidance addresses each of the money laundering issues for both of these two distinct areas.

- 13.3 Investors typically invest in a private equity fund vehicle as limited partners in a limited partnership and the private equity fund is represented by a general partner. The general partner usually appoints a private equity firm either to manage (in lieu of the general partner) or advise the private equity fund. Whilst the private equity fund will enter into transactions and have rights and obligations as regards portfolio companies, the AML responsibilities may reside with either the general partner of the private equity fund or with the private equity firm. The role and authority of the private equity firm is dependent on structure of the private equity fund. References throughout this sectoral guidance to “private equity firm” should be taken to include or make reference to a private equity fund as represented by its general partner (or other similar administrator), where the AML responsibilities reside with the private equity fund.

FINAL BOARD APPROVED

- 13.4 This sectoral guidance refers to “portfolio company” throughout. This may include a corporate group as a whole, a single entity or a company at the top of a corporate group. It may also include a company or group of companies which are the target of an intended investment, but which do not yet form part of the portfolio of a private equity fund. References to “portfolio company” should be interpreted according to the circumstances.

What are the money laundering risks in private equity?

- 13.5 Private equity firms are required to assess the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.
- 13.6 In carrying out their risk assessments, private equity firms should also have regard to Part I, paragraph 5.3.23, and Title II and Chapter 8 of Title III of the ESA Risk Factors Guidelines. The following may assist with a private equity firm's business-wide risk assessment.

Fundraising**Product risk**

- 13.7 Investors invest in a private equity fund for the long term and the timing of any return of capital is unpredictable. Minimum commitment sizes are usually very substantial and commitments are drawn down as required over the investment period of a fund at relatively short notice. This form of investment is also very illiquid with a limited ready market. Redemptions, withdrawals and transfers of interests in a partnership can take place, but usually only after the parties have conducted detailed due diligence and usually only with the specific approval of the fund's general partner or manager (and in some funds only after a minimum initial investment period). Payments/repayments would also only tend to be made to the fund investor itself (any payment to a third party would usually only be made with the express consent of the general partner or manager of the fund and the registered investor).
- 13.8 For the reasons stated in paragraph 13.7 above, an investment into a private equity fund would normally be considered to be a low risk product.

Customer risk

- 13.9 Investors in a private equity fund are mostly institutional, such as insurance companies, pension funds of large corporates or state organisations, Sovereign Wealth Funds, University Endowments, other financial services companies, charitable organisations and funds of funds. Investors may also include high net worth individuals typically investing through a ‘family office’.
- 13.10 The acceptance of investors into a private equity fund is a relatively long process with significant levels of due diligence performed by the private equity firm and a prospective investor and the final negotiation of key contracts that govern the relationship between the private equity fund and the investor. Key representatives of the prospective investor will normally meet face to face with senior executives of the private equity firm as part of this due diligence process. Investors will need to meet strict eligibility criteria to invest in private equity funds. The private equity firm has full discretion in admitting an investor to a fund and can decline a potential investor for any reason (including AML concerns).
- 13.11 It is not uncommon for a high proportion of investors to commit over a number of years to consecutive funds of the private equity firm; thus many investor relationships develop and continue over many years, often decades.
- 13.12 For the reasons set out in paragraphs 13.10 and 13.11, fund investors would generally be considered to be low risk, although certain investors may require extra consideration in any risk

FINAL BOARD APPROVED

evaluation - for example, where the investor is based in, or the funds to be invested are paid from an account in a high-risk third country (see Part I, paragraph 5.5.11).

- 13.13 Private equity firms seeking to raise funds for the first time, or from a significantly larger or less institutional investor base, may be considering accepting funds from potentially higher risk investors, and the extent of the due diligence should be adapted accordingly.

Transactions**Product risk**

- 13.14 The product is considered to be the provision of finance by a private equity fund that is operated, managed or advised by a private equity firm to predominantly unquoted companies. The funding can take place in a variety of ways and is usually provided for the long term after the portfolio company and its management have been subject to detailed due diligence. The private equity firm has an ongoing obligation to its investors to monitor its fund portfolio companies and will typically receive regular financial and operational information. The private equity fund will typically request the right to representation on the board of the portfolio company (this will usually be one or more of the executives from the private equity firm that manages or advises the fund but may be an external candidate chosen by the private equity firm for their relevant industry experience). The private equity fund will also typically have the right to attend portfolio company board meetings as an observer either instead of or in addition to the right to appoint a director.
- 13.15 The private equity fund's shareholding in a portfolio company is often highly visible and any failings on the part of the portfolio company are closely aligned to the reputation of the private equity firm.
- 13.16 If many of these factors are present it is considered unlikely that the provision of funding will be used for illegal purposes and therefore the product is low risk. The absence of certain of these factors, such as the absence of detailed due diligence work and/or the absence of customary investor protections, may require the private equity firm to conduct more detailed verification to satisfy itself that the financing being provided by the private equity fund is for legitimate purposes.

Customer risk

- 13.17 The range of portfolio companies invested in is determined by the specific parameters of the private equity fund as agreed with the fund investors. The level of regulation and standard of controls governing each portfolio company can vary considerably. The private equity firm's due diligence process should identify the risk profile of a prospective portfolio company and the private equity firm should consider its AML/CTF approach to that portfolio company accordingly.
- 13.18 Private equity investment is frequently provided to corporate groups whose operations span a number of different jurisdictions. The jurisdiction(s) in which a portfolio group operates may increase the money laundering risk profile, even if the parent is incorporated or registered in a well-regulated jurisdiction. A private equity firm would need to adapt its AML/CTF approach accordingly.
- 13.19 Likewise, the business sector(s) in which a portfolio company is engaged should be assessed from the perspective of money laundering risk. Certain sectors/businesses are more likely to be a target for money launderers than others, and the approach to due diligence should be adapted accordingly.
- 13.20 There will always be an obligation for a private equity firm to carry out such investigative work as it feels necessary where any circumstances exist which may lead it to suspect money

FINAL BOARD APPROVED

laundering or terrorist financing is a risk, and the following guidance should be read in that context.

Who is the customer for AML purposes?

13.21 For AML purposes, the “customer” is considered to be a party with whom a private equity fund is transacting on an occasional basis or a party with whom a private equity fund establishes a business relationship. Although these parties are referred to as “customers” for AML purposes, they are not parties that a private equity firm would typically consider to be “customers” from a regulatory perspective. In a private equity context there are two distinct groups of AML “customers”:

- **Fundraising:** Investors in private equity fund vehicles operated, managed or advised by private equity firms.
- **Transactions:** Persons transacting with a private equity fund operated, managed or advised by the private equity firm when making, managing and exiting from investments (e.g. portfolio companies, purchasers and sellers of portfolio companies and co-investors).

Customer due diligence

Fundraising

Identification of customer

13.22 In relation to each fund investor, a private equity firm should refer to the guidance for that type of investor in Part I, Chapter 5.

Identifying the beneficial owner

- 13.23 Where the investor is a natural person or a wholly-owned investment vehicle of a natural person, the firm should be able to identify and take reasonable measures to verify the identity of the beneficial owner.
- 13.24 Where the investor is a family office, the money will usually be provided by one or more trusts. The private equity firm should look through the investment structure to identify the relevant trusts, and verify the trusts’ identities in accordance with Part I, paragraphs 5.3.246 – 5.3.261. A private equity firm may have to take a decision as to whether it can rely on a representation from the administrator of the family office (or equivalent), or the trustees, as applicable, concerning the beneficial owners, or in appropriate cases confirmation from a reputable professional services firm. The amount and type of documentation collected will vary depending upon the firm’s risk-based approach.
- 13.25 Where the investor is a pension fund or endowment, the private equity firm must first understand the structure of the pension fund or endowment in order to determine its approach to identification. The private equity firm should identify both the source of the funding, for example the sponsoring employer, and the person who controls the investment decision, for example the trustee or an investment committee, although the exercise of investment discretion may have been delegated to a regulated firm acting as agent. The private equity firm should identify and take reasonable measures to verify the identity of any beneficial owners of the pension scheme or endowment.
- 13.26 The guidance in paragraphs 13.49 to 13.54 is relevant for customer due diligence relating to investing corporates.
- 13.27 It may be more complicated to identify a beneficial owner where the investor is itself a fund vehicle, for example a private equity fund of funds. The guidance in paragraphs 13.55 to 13.69 is relevant for customer due diligence relating to investing funds.

FINAL BOARD APPROVED**Timing of customer due diligence**

- 13.28 Identification checks in respect of investors in a fund should be completed and the private equity firm satisfied as to the source of funds before any unconditional contractual commitment to accept the investor into the fund is made. Where there is any assignment of an interest in a fund, any identification checks should be completed before the assignment is approved and executed.

Transactions

- 13.29 There are a number of parties involved in a private equity transaction, and the level of identification required in respect of each will vary, depending on the type of transaction, the nature of the party and their role in the transaction and how well they may already be known to the private equity firm.

New investments

- 13.30 On a new investment a private equity firm should consider applying customer due diligence measures, adopting a risk-based approach, to the following counterparties (each of which is explained in further detail below):

- the portfolio company;
- potentially, any new company formed for the purposes of making the investment;
- any party who is selling shares to either the private equity fund or a new company formed for making the investment; and
- potentially, a party making a co-investment alongside the private equity fund.

- **Portfolio companies**

- 13.31 Where the investment is provided directly to a company, customer due diligence in accordance with Part I, Section 5.3.122 onwards should be applied to that portfolio company.
- 13.32 Beneficial owners of the portfolio company must be identified and the private equity firm must take reasonable measures to verify their identity. These are often the same parties identified as part of the customer due diligence undertaken on the sellers where the private equity investment is being used to fund an exit by existing shareholders.
- 13.33 One or more new special purpose vehicles (“newcos”) may be used for the purposes of the transaction. This means that the private equity firm or its funds may only enter into a direct transaction with a newco and not the portfolio company. Nevertheless, the investment funds will ultimately be flowing down to the portfolio company in linked transactions so there must be a clear understanding of the underlying beneficial ownership or recipient of the funds and the flow of financing. For this reason, customer due diligence should be conducted on the portfolio company to be acquired by a newco. See paragraphs 13.37 and 13.38 for guidance on the customer due diligence requirements in relation to newcos.
- 13.34 Where the investment is provided to a corporate group (whether directly or indirectly through one or more newcos), customer due diligence should be applied to the top entity within the corporate group that is being acquired or that is receiving the private equity investment, as it existed prior to imposition of any newcos. Where the corporate group receiving the investment is being ‘carved out’ from a larger corporate group, customer due diligence should be applied to the top company of the grouping being carved out, prior to the imposition of any newcos.
- 13.35 A private equity firm must consider and understand the ownership and control structure of the portfolio group as a whole.

FINAL BOARD APPROVED

- 13.36 The private equity firm will obtain and verify the names of all board directors of the portfolio company as part of the standard evidence for a corporate in accordance with Part I, paragraph 5.3.129. The private equity firm should consider whether to verify the identity of one or more directors in accordance with Part I, paragraph 5.3.146.

- **Newcos**

- 13.37 One or more newcos may be used for the purposes of the transaction, either to acquire the target portfolio group or for the purposes of efficient tax structuring. Newcos are typically formed by the private equity firm or professional advisers representing any of the private equity firm, a lead co-investor or investing management. The initial directors and shareholders of such newcos will usually be connected to the private equity firm or the professional adviser and will be changed before or at signing. Assuming this to be the case, where any newco has not previously traded and was formed in anticipation of a transaction, there should be no reason to carry out formal customer due diligence on any newco. The jurisdiction of the newco may carry a higher risk profile, but provided that the newco has been properly established and that the reason for the selection of jurisdiction is understood and appropriate, that of itself should not give rise to the need to obtain additional verification. Where any newco does not meet these criteria, customer due diligence measures may be appropriate according to a private equity firm's assessment of the risks.
- 13.38 Where the transaction introduces a chain of newcos, it should only be necessary to consider customer due diligence (if any, as per paragraph 13.37 above) with respect to the top newco in the proposed corporate structure, into which the private equity firm or its funds is investing, assuming that the newcos below will all be wholly-owned by the top newco and that all directors are representatives of the private equity firm or co-investors or are known from within the portfolio group or will be changed before or at signing to such directors.

- **Sellers**

- 13.39 The decision to invest by the private equity firm may be used to fund an exit by existing shareholders, resulting in one or more individuals or entities benefiting financially.
- 13.40 Sellers of a portfolio company will be customers of the private equity fund for AML purposes where they are transacting directly with the private equity fund. A private equity firm should identify all sellers and adopt a risk-based approach to the extent of the measures taken to verifying the identity of sellers (and any beneficial owners), according to the firm's assessment of the money laundering risk presented by each seller. Even if the placement of newcos in the structure means that there is no direct transaction between the private equity fund and any sellers, the private equity firm should conduct customer due diligence on the sellers given that all or part of the benefit of the private equity investment is flowing to them. The nature of the due diligence work performed is such that the origins of the business will have been the subject of extensive review and investigation.
- 13.41 The guidance in paragraphs 13.49 to 13.54 is relevant for customer due diligence relating to selling corporates.
- 13.42 The guidance in paragraphs 13.55 to 13.69 is relevant for customer due diligence relating to selling funds.

- **Co-investors**

- 13.43 Private equity transactions can involve a variety of co-investors. These might include other private equity funds, institutional investors (who may also be invested in the private equity fund alongside which they are co-investing), incoming directors or managers, or existing founders /

FINAL BOARD APPROVED

managers / employees of a business who are continuing (or ‘rolling over’) their investment in a portfolio company or being provided with a new opportunity to co-invest. Depending on the circumstances, a private equity firm should consider whether to identify co-investors, particularly in the following circumstances:

- Where the private equity fund acts as lead investor in the round of financing where it has arranged a co-investor’s involvement in the deal, and where the co-investor is formally relying on the private equity fund, as can be the case in venture financing rounds or club deals; or
- Where a co-investor is taking a significant stake of the investment, alongside the private equity fund, so that it becomes a beneficial owner of the portfolio company; or
- When a co-investor is an individual and is or will be a board director of the portfolio company.

13.44 A private equity firm should adopt a risk-based approach to verifying a co-investor’s identity according to the firm’s assessment of the money laundering risk presented by a co-investor. The guidance in paragraphs 13.55 to 13.69 is relevant for customer due diligence relating to co-investing funds.

Further investments

13.45 On a further or follow-on investment in a portfolio company, a private equity firm should consider whether its ongoing monitoring of the portfolio company (see paragraph 13.78 onwards) has been sufficient for AML purposes or whether it would be appropriate to update its customer due diligence on the portfolio company. It should not be necessary to re-verify or obtain current documentation unless the identification data held is not adequate for the risk of the business relationship or there are doubts about the veracity of the information already held. The same considerations apply to any co-investors also making a further investment or new commitment.

Timing

13.46 Customer due diligence checks should generally be completed when it is reasonably certain that the new or further investment will go ahead, and in all cases before the private equity fund becomes unconditionally legally obliged to complete the investment.

Realisations

13.47 When realising an investment in a portfolio company (either fully or partially) the private equity firm should consider applying customer due diligence measures, adopting a risk-based approach and depending on the nature of the exit as follows:

- On a private sale, the purchaser of the portfolio company;
- On an IPO, the lead underwriters in the underwriting agreement;
- On a buy back, either on the purchasing managers or the portfolio company itself depending on who is buying back the shares.

- **Purchasers**

13.48 The pressures of achieving a timely and successful exit may heighten the risk of limiting the amount of due diligence performed on any potential purchaser on exit. In these circumstances the private equity firm needs to ensure that its controls for proper verification of identity and establishing source of funding remain robust.

FINAL BOARD APPROVED

- **Transacting with corporates**

- 13.49 Where the purchaser is a corporate entity the private equity firm should apply customer due diligence measures in accordance with Part I, Section 5.3.143 onwards.
- 13.50 Where a purchaser establishes a newco to make the acquisition, customer due diligence should identify those directors and beneficial owners who will ultimately own and control newco when the transaction completes, rather those who formed newco. If ownership of newco will change between signing and closing, a private equity firm may need to identify those in place at signing as well as closing.
- 13.51 In a corporate structure, beneficial ownership may be exercised through a direct holding or through several intermediate investment vehicles. A private equity firm must understand the ownership and control of the corporate structure to which the purchaser belongs and identify the names of all individual beneficial owners, even where these interests are held indirectly, whether through one or multiple vehicles. Enquiries should continue up the chain of ownership until either any natural persons who are beneficial owners of the purchaser are encountered or it is established that no such individual exists (for example, as may be the case with a company whose ultimate parent is listed on a regulated market).
- 13.52 Beneficial ownership should be considered on a look-through basis. If one individual appears in several different places within a corporate structure, that individual may have effective beneficial ownership of the purchaser as a consequence of the aggregated holdings exceeding the 25% threshold. Conversely, an individual owning or controlling more than 25% of a company at the top of a corporate structure is not necessarily a beneficial owner of the transacting purchaser if he does not have effective control or ownership of more than 25% of the transacting purchaser because of the dilutive effect of intermediate companies which are not wholly-owned and is not otherwise an individual who exercises control over the management of the company. For example, Individual A who owns/controls 30% of Company B (which in turn owns/controls 40% of Company C) is not necessarily a beneficial owner of Company C as Individual A's effective ownership/control of Company C is diluted to 12% (i.e. 30% of 40%).
- 13.53 If a private equity firm has exhausted all possible means of identifying the beneficial owner of the corporate entity and it has not been able to do so or has doubts as to whether the individual it has identified is in fact the beneficial owner, it may treat the senior person(s) responsible for managing the purchaser as the beneficial owner. However, if it does this, the firm must nonetheless keep records of all the actions it took in attempting to identify the beneficial owner.
- 13.54 Where there is a series of corporates in the ownership chain, which ultimately ends with a beneficial owner, the private equity firm must take reasonable measures to verify the identity of any such beneficial owner. There is no need to verify the identity of all entities in the intermediate ownership layers, although the private equity firm should retain suitable evidence of all intermediate ownership layers and relevant ownership percentages.

- **Transacting with funds**

- 13.55 It is reasonably common to encounter private equity (or similar) funds as counterparties in private equity transactions.
- 13.56 In the UK, fund vehicles are typically formed as limited partnerships. Limited partnerships are registered at Companies House and have a registration number and a registered address. In other jurisdictions, funds may be in the form of partnerships or corporate vehicles. Funds will normally have a general partner or a manager who exercises discretion over the assets of the fund. In these paragraphs "Fund Manager" refers to this entity/person, regardless of form or title.

FINAL BOARD APPROVED

- 13.57 A private equity firm must conduct customer due diligence on a fund, as set out in Part I, Chapter 5 according to the form of the fund vehicle. This may be achieved, subject to the firm's risk assessment and the considerations outlined below, by way of reliance on representations from its Fund Manager (see paragraphs 13.61 to 13.68).
- 13.58 Customer due diligence, whether by way of reliance on representations or directly obtaining standard evidence, must identify all purchasing funds and any beneficial owners. Part of the process of identifying the beneficial owners of the fund may include establishing the name of the Fund Manager given its ability to control the fund assets. A private equity firm will also need to identify and take reasonable measures to verify any beneficial owner, including any natural person who owns or controls an interest in excess of 25% of the fund.
- 13.59 If a private equity firm conducts customer due diligence directly (either instead of or to supplement a Fund Manager's representations (see below)) it may obtain other items of standard evidence, for example basic constitutional or incorporation documents in relation to the fund vehicle and its Fund Manager and evidence of the Fund Manager's regulated status (if relevant).
- 13.60 A private equity firm may accept representations from the Fund Manager (subject to paragraphs 13.61 – 13.67 below) to fulfil some or all of its customer due diligence requirements as regards the identity of the funds, its Fund Manager and the Fund Manager's regulated status and to establish whether or not there are any investors in the fund that are beneficial owners. Funds are often widely held and it may be the case that no investor is a beneficial owner.
- 13.61 Where a fund does have beneficial owners who must be identified and whose identity should be verified, there will often be legitimate confidentiality concerns on the part of the Fund Manager with respect to investors in the fund. A private equity firm must take reasonable measures to verify identity. A private equity firm may consider it appropriate, depending on its knowledge and assessment of the Fund Manager and applying a risk-based approach, to rely on a representation from the Fund Manager that it has verified a beneficial owner's identity and will provide documentary evidence immediately upon request.
- 13.62 Where the Fund Manager is established in a high-risk third country (see Part I, paragraph 5.5.11), a private equity firm should not rely on representations from the Fund Manager relating to the satisfaction of customer due diligence requirements and must consider whether it is able otherwise to satisfy its customer due diligence requirements.
- 13.63 Subject to the firm's risk assessment, where the Fund Manager is regulated and subject to supervision in the UK or the EU, it will be subject to the requirements of the ML Regulations or equivalent and a private equity firm is entitled to rely on such a Fund Manager's representation relating to the satisfaction of customer due diligence requirements. These representations may take the form of a letter or similar from the Fund Manager as outlined below (see paragraphs 13.67 and 13.68).
- 13.64 Subject to the firm's risk assessment, where the Fund Manager is not in the UK or the EU, but the Fund Manager is:
- a. established in a jurisdiction that is not a high-risk third country (see Part I, paragraph 5.5.11);
 - b. subject to requirements in relation to customer due diligence and record keeping which are equivalent to those laid down in the fourth money laundering directive; and
 - c. supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter VI of the fourth money laundering directive,

FINAL BOARD APPROVED

the private equity firm may also rely on a letter or similar from the Fund Manager setting out representations (see paragraphs 13.67 and 13.68).

- 13.65 Where the Fund Manager is not in the UK or the EU, is not established in a jurisdiction that is a high-risk country (see Part I, paragraph 5.5.11) but does not satisfy each of the conditions in paragraphs 13.64 b and c above, the private equity firm may not rely on that Fund Manager to apply any of the customer due diligence measures required but may, exercising its judgement as part of a risk-based assessment, accept certain confirmations from the Fund Manager - for example in the situation referred to in paragraph 13.69 below. Factors to take into consideration in making this risk-based assessment include:
- whether the Fund Manager is regulated or unregulated;
 - the countries and geographic areas section of the ESA Risk Factors Guidelines;
 - the Fund Manager's willingness to explain its identification procedures and provide confirmation that all underlying investors in the fund have been identified and are known to the Fund Manager;
 - the profile of the Fund Manager in the market place; and
 - the Fund Manager's track record in the private equity industry.
- 13.66 Notwithstanding a private equity firm's reliance upon or acceptance of Fund Manager representations, the private equity firm will remain liable for non-compliance and it may not always be appropriate to rely on another Fund Manager to undertake its customer due diligence checks.
- 13.67 Representations from a Fund Manager should confirm the name and jurisdiction of the fund, that the Fund Manager acts as the manager for the fund, whether or not the Fund Manager is regulated, that the Fund Manager has carried out due diligence on the fund investors and whether there is a natural person who is a beneficial owner of the fund and, if so, the name of that person.
- 13.68 A possible example of a letter of representations as referred to in paragraphs 13.63 to 13.67 is set out below:

Example of letter of representations provided by a Fund Manager

"We [*name of firm*] [regulated by [*name of regulator and firm reference number if any*]] confirm the following in respect of [*name, business address and, if applicable, registered number of fund vehicle(s)*] (the "Fund(s)"), established in [*fund jurisdiction(s)*] for whom we act as manager/general partner.

1. [In accordance with the laws of our jurisdiction, and the procedures under which we operate, designed to combat money laundering] we confirm that:
 - we have carried out customer due diligence on all of the investors in the Fund(s);

FINAL BOARD APPROVED

- we confirm that to our actual knowledge [(having made reasonable enquiries)] there are no undisclosed or anonymous principals; and
 - we are not aware of any activities on the part of those investors which lead us to suspect that the investor is or has been involved in money laundering or other criminal conduct.
2. To our actual knowledge [(having made reasonable enquiries)] [there is no natural person who ultimately is entitled to or controls (in each case whether directly or indirectly) more than a 25% share of the capital or profits of the Fund(s) or more than 25% of the voting rights of the Fund(s)] OR [*insert identity of any natural persons who ultimately is entitled to or controls 25% of capital, profits or voting rights*] is a beneficial owner of the Fund(s);
3. [No single individual exercises control over the management of the Fund.] [OR] [*Name of individual* exercises control over the management of the Fund].
4. We will:
- provide [you] OR [your Compliance Officer] with copies of any identification and verification data and any other relevant documentation on the identity of the Fund(s), the investors and beneficial owner(s) of the Fund(s) immediately on request; and
 - retain copies of the data and documents referred to above and sufficient supporting records in respect of all transactions involving the Fund(s) for at least five years from the end of the business relationship with the Fund(s).
- 13.69 In certain circumstances, where the private equity firm needs to carry out customer due diligence on a corporate entity as customer (such as a target portfolio company or holding company seller) that corporate entity will be (wholly or partly) owned by a fund. In addition to applying customer due diligence measures in respect of the corporate entity and taking reasonable measures to understand its ownership and control structure in accordance with Part I, paragraph 5.3.143 onwards, the private equity firm must identify whether there are any beneficial owners, and if so, take reasonable measures to verify their identity. In order to determine whether there are any natural persons who have an ownership interest in the fund that would make them an ultimate beneficial owner of the corporate entity), the private equity firm may need to seek to rely on a confirmation from the relevant Fund Manager. In this regard, subject to considering the same issues referred to in paragraphs 13.63 to 13.65 (as to the Fund Manager's location and the basis on which it is supervised) and in paragraph 13.66 (as regards the private equity firm's liability for any non-compliance), the private equity firm may accept a letter or similar from the Fund Manager regarding beneficial owners. The status of such a letter or similar will depend on the issues referred to in paragraphs 13.63 to 13.65 but should confirm the name and jurisdiction of the fund, that the Fund Manager acts as the manager for the fund, whether or not the Fund Manager is regulated and whether there is a natural person who ultimately is entitled to or controls (directly or indirectly) more than a 25% share of the capital or profits of the fund or more than 25% of the voting rights of the fund and, if so, the name of that person.
- **Buy backs**
- 13.70 If the sale is to a member of existing management on whom customer due diligence was conducted at the outset or during the life of the investment and who has been known to the private equity firm in the context of the investment concerned (or of another investment), the

FINAL BOARD APPROVED

private equity firm should consider the relevance of carrying out further customer due diligence given its existing relationship with, and knowledge of, the member of management concerned.

- 13.71 If the portfolio company is funding the buyback, the company is the purchaser and the private equity firm should consider its existing relationship with the company and whether it has up to date knowledge of the portfolio company through its existing monitoring processes, in deciding whether it is necessary to refresh its customer due diligence.

- **IPOs**

- 13.72 On an IPO, where the private equity fund is able to sell some of its shares in the portfolio company, the private equity fund will typically be transacting with one or more lead underwriters. The private equity firm need not be concerned with sub-underwriters unless the contractual arrangements provide for the private equity fund to sell directly to them. The private equity firm should undertake customer due diligence on any lead underwriter. Since it will be a regulated firm, simplified due diligence may be appropriate, subject to carrying out a risk assessment and provided that they are not located in a high risk jurisdiction. Whether acting as agent or principal for the private equity fund in selling the shares, the lead underwriter will be subject to AML rules and will either sell the shares on a regulated market or through another broker, so the private equity firm need not concern itself with identifying the ultimate purchasers of the shares. The private equity firm would expect to see some acknowledgement of the lead underwriter's compliance with relevant AML rules in the underwriting agreement.
- 13.73 Where a private equity fund does not sell at the time of the IPO, there is no transaction or customer for AML purposes. Any later sale will trigger customer due diligence requirements although this will frequently be transacted through a regulated broker, where similar considerations to those in paragraph 13.72 will be relevant.

Timing

- 13.74 Identification checks should generally be completed on the relevant parties as soon as practicable when a deal looks reasonably likely to proceed and in all cases before the private equity fund becomes unconditionally legally obliged to complete the sale.

Other issues

Representations issued by private equity firms to third parties

- 13.75 A private equity firm should be prepared to confirm whether in its actual knowledge there are any beneficial owners in a private equity fund for which it has AML responsibilities. When disclosing information about investors this should be done in accordance with relevant confidentiality provisions, and private equity firms should consider agreeing to disclose the information to a certain department within the third party, such as the Compliance Officer, only. Such confirmations might be required by another party transacting with the private equity fund or, more commonly, by a bank funding a portfolio company that is conducting or refreshing its own customer due diligence on the portfolio company's beneficial owners.

Use of verification carried out by others

- 13.76 Private equity firms make extensive use of professional advisers, especially where the required knowledge does not exist in the private equity firm itself. A portfolio company and any co-investors will usually appoint professional advisers to ensure that their own interests are represented in any negotiation. In some cases, these advisers are themselves under an obligation under the ML Regulations, or under similar legislation in the EU or in another jurisdiction assessed as low risk, to carry out customer due diligence on their clients. Depending on the circumstances, and the private equity firm's knowledge of/relationship with the portfolio company, the private equity firm may consider it appropriate to take account of information or

FINAL BOARD APPROVED

written assurances provided to the private equity firm by these third parties, as part of the overall risk-based approach.

- 13.77 The requirement to appear before a notary in certain jurisdictions when signing documents such as the sale and purchase agreement or shareholders' agreement can provide adequate verification. However the notary's certificate should only be considered as adequate if it states the full names and identity card numbers (or equivalent) of the individuals appearing before the notary, plus details of the evidence provided for their authority to act as representatives of the parties involved.

Ongoing Monitoring

- 13.78 A private equity firm must conduct ongoing monitoring of "customers" (for AML purposes) with whom it establishes business relationships. Although a private equity firm may carry out customer due diligence on a wide variety of parties in the course of transactions, many of these are as a result of occasional transactions rather than any intention to establish a business relationship for AML purposes. In an AML context, private equity firms usually establish business relationships with fund investors and portfolio companies. Although private equity firms may make multiple investments alongside the same co-investors, the contractual nature of the arrangements between co-investors are bespoke for each investment and the relationship is not one for which a private equity firm is generally expected to conduct ongoing monitoring.
- 13.79 The extent of the ongoing monitoring must be determined on a risk sensitive basis but a private equity firm should bear in mind that as the business relationship develops, the risk of money laundering may change. It should not be necessary to re-verify or obtain current documentation unless the identification data held is not adequate for the risk of the business relationship or there are doubts about the veracity of the information already held, for example, where there is a material change in the risk profile of the customer.

Fundraising

- 13.80 Investors in private equity funds tend to have long established relationships with the private equity firm, normally resulting in a well-known investor base.
- 13.81 Private equity firms will have regular one-on-one meetings with representatives of their fund investors or may organise investor conferences to update them on the performance of their funds. The private equity firm will typically provide regular written reports to fund investors on the performance of a fund and its portfolio.
- 13.82 Fund investors regularly submit questionnaires to private equity funds asking them to confirm compliance with the fund's organisational documents and various aspects of the fund management policies and procedures and their house investment approach.
- 13.83 These activities are indicative of continuing dialogue and communication and should be considered sufficient ongoing monitoring of the relationship for AML purposes.

Transactions

- 13.84 Prior to making any investment in a business, the private equity firm will conduct extensive due diligence on the business and its owners, identifying areas of risk, including money laundering considerations. Once invested, ongoing monitoring of the investment through board participation and regular involvement allows the private equity firm to assess whether the portfolio company's activities are consistent with its financial performance, and also enables the private equity firm to observe the conduct of the key managers of the business at first hand. In connection with portfolio companies, this will satisfy a private equity firm's obligation to conduct ongoing monitoring of the business relationship for AML purposes.

14: Corporate finance

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in [Part I](#) of the Guidance.

This sectoral guidance considers specific issues over and above the more general guidance set out in Part I, Chapters 4, 5 and 7, which firms engaged in corporate finance activity may want to take into account when considering applying a risk-based approach to that sector. Firms may also find the following sectors useful:

- **Sector 13: *Private Equity***, which covers the private financing of companies.
- **Sector 18: *Wholesale Markets***, which covers the trading of securities in a primary or secondary market.

Overview of the sector

14.1 “Corporate finance” is activity relating to:

- The *issue of securities*. These activities might be conducted with an issuer in respect to itself, or with a holder or owner of securities. Examples include: arranging an initial public offering (IPO), a sale of new shares, or a rights issue for a company, as well as making arrangements with owners of securities concerning the repurchase, exchange or redemption of those securities;
- The *financing, structuring and management of a body corporate, partnership or other organisation*. Examples include: advice about the restructuring of a business and its management, and advising on, or facilitating, financing operations including securitisations;
- Changes in the *ownership of a business*. Examples include: advising on mergers and takeovers, or working with a company to find a strategic investor;
- Business *carried on by a firm for its own account* where that business arises in the course of activities covered by (i), (ii) or (iii) above, including cases where the firm itself becomes a strategic investor in an enterprise.

What are the money laundering risks in corporate finance?

14.2 As with any financial service activity, corporate finance business can be used to launder money.

14.3 The money laundering activity through corporate finance will not usually involve the placement stage of money laundering, as the transaction will involve funds or assets already within the financial system. However, corporate finance could be involved in the layering or integration stages of money laundering. It could also involve the concealment, use and possession of criminal property and arrangements to do so, or terrorist funding.

14.4 The money laundering risks associated with corporate finance relate to the transfer of assets between parties, in exchange for cash or other assets. The assets can take the form of securities or other corporate instruments.

FINAL BOARD APPROVED

How to assess the elements of risk in this sector

- 14.5 In order to forestall financial crime, including money laundering and terrorist financing, it is important to obtain background knowledge about all the participants in a corporate finance transaction, and not just those who are customers, who must be subject to customer due diligence. This background gathering exercise should include measures to understand the ownership and control structure of the customer as well as looking at the beneficial ownership and any possible involvement of politically exposed persons and establishing the purpose and intended nature of the business relationship and whether this is consistent with the transaction being undertaken.
- 14.6 In its assessment of the financial crime risk of a particular corporate finance transaction, a firm should use - where possible and appropriate - the information it has obtained as a result of the intensive due diligence it normally undertakes in any corporate finance transaction. This may include, but not be limited to, firms assessing the probity of directors, shareholders, and any others with significant involvement in the customer's business and the corporate finance transaction.
- 14.7 The money laundering risks associated with corporate finance activity can be mitigated if a firm understands or obtains assurances from appropriate third parties and/or the customer as to the source and nature of the funds or assets involved in the transaction. Firms should consider, on a risk based approach, the need to corroborate this information.
- 14.8 In addition, a firm should assess whether the financial performance of an enterprise is in line with the nature and scale of its business, and whether the corporate finance services it seeks appear legitimate in the context of those activities. The outcome of this assessment should be consistent with the purpose and intended nature of the business relationship.

*Who is the customer for AML purposes?**Issuer of securities*

- 14.9 Where a firm is facilitating the issue or offer of securities by an entity, that entity is the firm's customer.
- 14.10 In circumstances where vehicles are created for the purpose of issuing securities to investors e.g. Special Purpose Vehicles / Special Purpose Acquisition Company's (SPV, SPAC, respectively), the issuing SPV/SPAC will also be treated as a customer of the firm. These issuing SPVs or SPACs may often utilise "orphan" structures: they may ultimately be owned via a charitable trust or foundation which is discretionary in nature, with no ownership structure evident. In such situations, the economic beneficiary (i.e. the issuer) may not have an obvious equitable interest in the SPV/SPAC. However, the economic benefit flows might be evidenced by the offering memorandum.

In transactions where assets are consolidated into or contributed to SPVs (e.g. certain notes or obligations), the firm should consider the source of funds of these assets and the identity of those entities providing the assets for the SPV as this may be where the key ~~where~~ money laundering risk arises.

Purchaser of securities

FINAL BOARD APPROVED

14.11 Whether purchasers of the *securities* issued are customers for AML purposes will depend upon the relationship the firm has with them, and in particular whether or not a firm has behaved in a way that would lead the purchaser to believe that he is a customer. Therefore:

- A direct approach by a firm to a potential purchaser will create a customer relationship for the firm.
- Purchasers of securities may be deemed to be customers of the firm delivering the securities in settlement.
- A firm may, on a risk based approach, consider the investor identification measures adopted in the offering documentation.

Owners of securities

14.12 Where a firm advises the owners of *securities*, in respect of the repurchase, exchange or redemption by an issuer of those *securities*, the owners will be customers of the firm for AML purposes.

14.13 However, other than in exceptional cases, a firm may be precluded by other regulatory requirements from acting for both the issuer and the owners of the investments concerned. In the circumstances where a firm does act for the owners of the *securities*, the issuer will not generally be a customer of the firm for AML purposes.

Financing, structuring and management of a body corporate, partnership or other organisation

14.14 The entity with which a firm is doing investment business, whether by way of advice provided to the entity, or through engaging in transactions on its behalf, will be a customer of the firm for AML purposes.

14.15 The activity undertaken by a firm may entail the firm dealing in some way with other entities/parties on behalf of the customer entity, for example, through the sale of part of its customer's business to another entity or party. In these circumstances, the other entity or party whom the firm deals with on behalf of the customer will not also become the firm's customer as a result of the firm's contact with them during the sale. (For *Securitisations transactions* see paragraphs 14.30 – 14.36.)

Changes in the ownership of a business

14.16 The entity with which a firm is mandated to undertake investment business, whether by way of advice or through engaging in transactions, will be the customer of the firm for AML purposes.

14.17 Other entities or parties affected by changes in ownership, for example a takeover or merger target, will not become the firm's customers, unless a firm provides advice or other investment business services to that entity or party. Similarly, an approach by a firm to a potential investor on behalf of a customer does not require the firm to treat the potential investor as its customer for AML purposes, unless the firm provides advice or other investment business services to that investor.

Business carried on by a firm for its own account

14.18 Where a firm makes a principal investment in an entity, that entity will not be a customer of the firm. A principal investment in this context means an investment utilising the firm's capital and one that would not involve the firm entering into a business relationship within the meaning of the ML Regulations. If, as well as making a principal investment in an entity, a firm enters into a business relationship with that entity, for example, by providing investment services or

FINAL BOARD APPROVED

financing to the entity, the firm must apply the measures referred to in Part I, Chapter 5 as appropriate. When a firm has determined that the investment is not subject to the requirements of the ML Regulations, it may nevertheless wish to consider, in a risk-sensitive way, whether there are any money laundering implications in the investment it is making and may decide to apply appropriate due diligence measures.

Involvement of other regulated firms

14.19 A regulated firm (X) may be involved in a corporate finance transaction in which another regulated firm (Y) from an assessed low risk jurisdiction, is also involved. The relationship between X and Y may take a number of different forms:

- (a) X may be providing investment services to Y, for example, by facilitating an IPO for Y. In this case Y is the customer of X. X is not the customer of Y.
- (b) X and Y may both be providing investment services to a customer Z, for example by underwriting a private placement of shares for Z. In this case, Z is the customer of X and of Y. There is no customer relationship between X and Y.
- (c) X may be acting for an offeror (Z) in a takeover, and Y may be acting for the offeree (ZZ). Z is the customer of X and ZZ is the customer of Y. There is no customer relationship between X and Y.

14.20 A firm should establish at the outset whether it has a customer relationship with another regulated firm and, if so, should follow the guidance in [Part I, Chapter 5](#) in verifying the identity of that firm.

Customer due diligence

14.21 Corporate finance activity may be undertaken with a wide range of customers, but is predominantly carried on with listed and unlisted companies or their owners. The guidance contained in [Part I, Chapter 5](#) indicates the customer due diligence procedures that should be followed in these cases. However, the following is intended to amplify aspects of the [Part I, Chapter 5](#) procedures, with particular reference to the business practices and money laundering risks inherent in a corporate finance relationship.

Background information

14.22 It is necessary to look more closely than the procedures set out in [Part I, Chapter 5](#) for acceptance of the customer. It is important to check the history of the customer and to carry out reputational checks about its business and representatives and shareholders.

Timing

14.23 In corporate finance transactions, when a mandate or an engagement letter is signed is generally considered the point at which the firm enters into a binding relationship with the customer. Note, it is common for a firm to begin discussions with a customer before a mandate or engagement letter has been signed, and a firm may put in place indemnity or conditional commitment arrangements prior to agreeing any express mandate or engagement. Such arrangements may not constitute a binding customer relationship, as they are often designed to afford legal protections to the parties early on in a discussion and before the firm and its prospective customer(s) agree to a binding customer relationship.

FINAL BOARD APPROVED

- 14.24 A firm should determine when it is appropriate to undertake customer due diligence on a prospective customer and where applicable any beneficial owners. In all cases, however, the firm must ensure that it has completed appropriate customer due diligence once a binding customer relationship has been established.
- 14.25 Where, having completed customer due diligence, a mandate or engagement letter is not entered into until some time after the commencement of the relationship, a firm is not required to obtain another form of evidence confirming the customer's agreement to the relationship with the firm prior to the signing of the mandate, provided it is satisfied that those individuals with whom it is dealing have authority to represent the customer.
- 14.26 Whilst not an AML requirement, if the relationship is conducted, either initially or subsequently, with non-board members, the firm should consider satisfying itself at an early stage that the board has approved the relationship by seeking formal notification of the non-board members' authority to act on behalf of the company they represent.

Other evidence for customer due diligence

- 14.27 Where there is less transparency over the ownership of the customer, for example, where ownership or control is vested in other entities such as trusts or special purpose vehicles (SPV's), or less of an industry profile or less independent means of verification of the customer, a firm should consider how this affects the ML/TF risk presented. It will, in certain circumstances, be appropriate to conduct additional due diligence, over and above the firm's standard evidence. Firms have an obligation to verify the identity of all beneficial owners (see Part I, Chapter 5). It should also know and understand any associations the customer may have with other jurisdictions. It may also consider whether it should verify the identity of other owners or controllers. A firm may, subject to application of its risk-based approach, use other forms of evidence to confirm these matters. Consideration should be given as to whether or not the lack of transparency appears to be for reasonable business purposes. Firms will need to assess overall risk in deciding whether the "alternative" evidence, which is not documentary evidence as specified in [Part I, Chapter 5](#), is sufficient to demonstrate ownership and the structure as represented by the customer.
- 14.28 Firms should maintain file notes setting out the basis on which they are able to confirm the structure and the identity of the customer, and individuals concerned, without obtaining the documentary evidence set out in [Part I, Chapter 5](#). Such notes should take account of:
- Social and business connections
 - Meetings at which others are present who can be relied upon to know the individuals in question
 - The reliance which is being placed on banks, auditors and legal advisers

Subsequent activity for a customer

- 14.29 Some corporate finance activity involves a single transaction rather than an ongoing relationship with the customer. Where the activity is limited to a particular transaction or activity, and the customer subsequently engages the firm for other activity, the firm should ensure that the information and customer due diligence it holds are up to date and accurate at the time the subsequent activity is undertaken.

Securitisation transactions

FINAL BOARD APPROVED

- 14.30 Securitisation is the process of creating new financial instruments by pooling and combining existing financial assets, which are then marketed to investors. A firm may be involved in these transactions in one of three main ways in the context of corporate finance business:
- (i) as advisor and facilitator in relation to a customer securitising assets such as future receivables. The firm will be responsible for advising the customer about the transaction and for setting up the special purpose vehicle (SPV), which will issue the asset-backed instruments. The firm may also be a counterparty to the SPV in any transactions subsequently undertaken by the SPV;
 - (ii) as the owner of assets which it wants to securitise;
 - (iii) as counterparty to an SPV established by another firm for its own customer or for itself - that is, solely as a counterparty in a transaction originated by an unconnected party.
- 14.31 As a general rule, the firm should be more concerned with the identity of those who provide the assets for the SPV, as this is the key money laundering risk. So long as the firm demonstrates the link between the customer and the SPV, the SPV is not subject to the full requirements of [Part I, Chapter 5](#). However, the firm should obtain the basic identity information and hold evidence of the SPV's existence.
- 14.32 Whether a purchaser of the instruments issued by the SPV will be treated as customers will depend upon the relationship the firm has with them. Purchasers of instruments issued by the SPV arranged by a firm will not be customers of the firm so long as their decision to purchase is based on offering documentation alone, or on advice they receive from another firm, who will have a customer relationship with them. However, as part of a firm's risk-based approach, and for reputational reasons, it may also feel it appropriate to undertake due diligence on those who are purchasers of the instruments issued by the SPV.
- 14.33 In addition to verifying the identity of the customer in line with normal practice for the type of customer concerned, the firm should satisfy itself that the securitisation has a legitimate economic purpose. Where existing internal documents cannot be used for this purpose, file notes should be made to record the background to the transaction.
- 14.34 The firm needs to follow standard identity procedures as set out in Part I, paragraphs 5.3.69 to 5.3.293 with regard to the other customers of the firm to which it sells the new instruments issued by the SPV it has established.
- 14.35 If the firm is dealing with a regulated agent acting on behalf of the SPV, it should follow normal procedures for dealing with regulated firms.
- 14.36 If the firm is dealing with an unregulated agent of the SPV, both the agent and the SPV should be identified in accordance with the guidance in Part I, paragraph 5.3.71. Background information, obtainable in many cases from rating agencies, should be used to record the purpose of the transaction and to assess the money laundering risk.

Monitoring

- 14.37 The money laundering risks for firms operating within the corporate finance sector can be mitigated by the implementation of appropriate, documented, monitoring procedures. General guidance on monitoring is set out in Part I, section 5.7.

FINAL BOARD APPROVED

- 14.38 Monitoring of corporate finance activity will generally, due to the relationship-based, rather than transaction-based (in the wholesale markets sense), nature of corporate finance, be undertaken by the staff engaged in the activity, rather than through the use of electronic systems.
- 14.39 The essence of monitoring corporate finance activity involves understanding the rationale for the customer undertaking the transaction or activity, documenting the intended use of proceeds, and the staff using their knowledge of the customer, the rationale for the transaction or activity and the intended use of proceeds and what would be normal in the given set of circumstances, and using that information to spot the unusual or potentially suspicious.
- 14.40 The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:
- Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;
 - Adequacy of staff training and awareness;
 - Capturing appropriate management information;
 - Upward reporting and accountability; and
 - Effectiveness of liaison with regulatory and law enforcement agencies.

The responses to these matters need to be documented in order to demonstrate how it monitors and improves the effectiveness of its systems and procedures.

- 14.41 The firm will have ongoing relationships with many of its customers where it must ensure that the documents, data or information held are kept up to date. Where, as is likely in some cases with corporate finance activities, the customers may not have an ongoing relationship with the firm, it is important that the firm's procedures to deal with new business from these customers is clearly understood and practised by the relevant staff. It is a key element of any system that up to date customer information is available as it is on the basis of this information that the unusual is spotted, questions asked and judgements made about whether something is suspicious.

15: Trade finance

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance Note.

Firms addressing the money laundering/terrorist financing risks in trade finance should also have regard to the guidance in sector 16: Correspondent Relationships.

Overview of the sector

- 15.1 'Trade Finance' is used to describe various operations, including the financing – usually but not exclusively by financial institutions - undertaken to facilitate trade or commerce, which generally involves the movement of goods and services between two points – it can therefore be domestic or international. The trade finance element may only be part of the overall financial component and may have multiple variations, e.g., a domestic trade finance transaction could support an international movement of goods, or on occasion only services may be involved (see paragraph 15.9: Funds transmission/payments). Such operations comprise a mix of money transmission instruments, default undertakings and provision of finance, which are described in more detail below. A glossary of trade finance terms used in this guidance is set out in Annex 15-I.
- 15.2 In the context of this guidance, the term 'Trade Finance' is used to refer to the financial component of an international trade transaction, i.e., managing the payment for goods and/or related services being imported or exported. Trade finance activities may include issuing letters of credit, standby letters of credit, bills for collection or guarantees. Trade Finance operations are often considered in a cross-border context but can also relate to domestic trade.
- 15.3 Past estimates suggest that approximately only a fifth of world trade is conducted by means of trade finance products and services; the rest is conducted on "Open Account" terms, whereby a 'clean' payment is made by the buyer of the goods or services direct to the seller, i.e., not requiring presentation of the supporting trade documentation to the banks through which the payment is effected. It follows that whenever credit and liquidity are scarce or trust between the transacting parties has not been established, sellers in particular will be inclined to revert to Trade Finance.
- 15.4 In Open Account transactions, unlike transactions where trade finance instruments are used, the bank is only aware of the payment and will not be aware of the reason for the payment, unless the relevant details are included in the associated SWIFT messages. Banks will therefore be able to carry out sanctions screening only on the payment, with anti money laundering checks achieved to the extent practicable by its risk-based transaction monitoring. Where credit is being provided, however, the bank may have more information to enable it to understand the reasons for the transaction and the financial movements. Banks are not required to investigate commercial transactions outside their knowledge, although if documentation they see as part of the banking transaction gives rise to suspicion, they should submit a SAR to the NCA, and seek consent, as appropriate.
- 15.5 The focus of this guidance is on those standard products used for the finance of the movement of goods or services across international boundaries. The products are:
 - Documentary Letters of Credit (LCs) and

FINAL BOARD APPROVED

➤ Documentary Bills for Collection (BCs).

These standard products have trade related documents (invoices, transport documents etc) that are sent through financial institutions and are examined by documentary checkers within the financial institution for consistency with the terms of the trade transaction. Such operations are illustrated (in simple terms) in Annex 15-II, and are described in more detail below.

- 15.6 These products are governed internationally by sets of rules of practice issued by of the International Chamber of Commerce (ICC). The ICC rules governing BCs are fundamentally different from the ICC rules governing LCs. The checks, which have to be made within limited timeframes by the financial institution (Collecting or Presenting bank, see below), on BCs are limited to determining that the documents received appear to be as listed in the collection instruction.
- 15.7 International trade finance transactions will usually involve financial institutions in different locations, acting in a variety of capacities. For the purpose of LCs these may include an Issuing Bank, an Advising Bank, Nominated Bank, Confirming Bank or Reimbursing Bank. For BCs there will be a Remitting, Collecting or Presenting Bank. The nature of the capacity in which a financial institution may be involved is important, as this will dictate the nature and level of information available to the financial institution in relation to the underlying exporter/importer, the nature of trade arrangements and transactions. The fragmented nature of this process, in which a particular financial institution may of necessity have access only to limited information about a transaction, means that it may not be possible for any one financial institution to devise hard coded rules or scenarios, or any patterning techniques in order to implement a meaningful transaction monitoring system for the whole transaction chain.
- 15.8 The main types of trade finance operations are described in more detail below. Whilst they are addressed separately, they are not necessarily mutually exclusive and these operations may be combined in relation to a single transaction, series of transactions or, on occasion, in relation to a particular project. In terms of assessing risk, it is important to understand the detailed workings of individual operations/financial instruments, rather than automatically assuming that they fit into a particular category simply because of the name that they may have been given.

Funds Transmission/Payments

- 15.9 Trade finance operations often involve transmission of funds where the payment is subject to presentation of document(s) and/or compliance with specified condition(s). Financing may on occasion be provided either specifically related to the instrument itself, or as part of a general line of credit.

Default Undertakings

- 15.10 As the term implies, such undertakings normally only involve payment if some form of default has occurred. Typical undertakings in this category are bonds, guarantees, indemnities and standby letters of credit. Provision of finance is less common than with funds transmission/payment instruments, but could also occur.

Structured Financing

- 15.11 This category comprises a variety of financing techniques, but with the common aim of facilitating trade and commerce, where financing is the primary operation, with any associated Trade Finance instrument and/or undertaking being subsidiary. On occasion, such financing may be highly complex e.g., involving special purpose vehicles (SPVs). Finance may be

FINAL BOARD APPROVED

provided against evidence of performance under a trade contract, often on a staged basis that represents progress in that contract.

What are the financial crime risks in Trade Finance?

General

15.12 A key risk around trade finance business is that seemingly legitimate transactions and associated documents can be constructed simply to justify the movement of funds between parties, or to show a paper trail for non-existent or fraudulent goods. In particular, the level and type of documentation received by a firm is dictated principally by the applicant or instructing party, and, because of the diversity of documentation, firms may not be expert in many types of the documents received as a result of trade finance business (although experienced trade finance staff should have a good understanding of the most commonly used types of document). Such a risk is probably greatest where the parties to an underlying commercial trade transaction are in league to disguise the true nature of a transaction. In such instances, methods used by criminals to transfer funds illegally range from over and under invoicing, to the presentation of false documents or spurious calls under default instruments. In more complex situations, for example where asset securitisation is used, trade receivables can be generated from fictitious parties or fabricated transactions (albeit the use of asset securitisation in trade finance is a very limited activity). The use of copy documents, particularly documents of title, should be discouraged, and should raise a due diligence query, except where the location of the original documents (of title) and the reasons for their absence is disclosed to and acceptable by the banks in the transaction. Banks should implement additional safeguards with respect to related party transactions, e.g. requiring further escalation and scrutiny, requesting documentary evidence to verify the authenticity, and understand the role of the related party(ies) in the transaction. Red flags relating to related party transactions include:

- Transaction is between or involves related parties
- Same address used for different transacting parties, usage of registered agent's address, or other address inconsistencies
- Unexplained or unnecessary parties to the transaction and who appear evasive about their identity/role on further enquiries
- Transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction
- Payment or payment requests of proceeds to a third party unrelated to the customer.

15.13 A form of trade finance is generally used instead of clean payments and generic lending to provide additional protection for the commercial parties and independent and impartial comfort when parties require some level of performance and payment security or when documentation is required for other purposes e.g., to comply with Customs, other regulatory requirements, control of goods and/or possible financial institution requirements. The key money laundering/terrorism risks arise when such documentation is adapted to facilitate non-genuine transactions, normally involving movement of funds at some point. A third party documentary letter of credit ("3rd Party LC") is a product whereby the bank issues an authenticated undertaking that represents a commitment to pay a beneficiary a specified amount of money against documents presented that comply with the terms and conditions as specified. The key difference from a regular LC is that the 3rd party is named as the "ordering party" as per the instruction of an existing client.

15.14 The Financial Action Task Force (FATF), regulators and others have identified misuse of the trade system as one of the methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the legitimate

FINAL BOARD APPROVED

economy. FATF typologies' studies indicate that criminal organisations and terrorist groups exploit vulnerabilities in the international trade system to move value for illegal purposes. Cases identified included: illicit trafficking in narcotic drugs; illicit trafficking in stolen or other goods; corruption and bribery; fraud; counterfeiting/piracy of products; and smuggling. More complicated schemes integrate these fraudulent practices into a complex web of transactions and movements of goods and money.

Money laundering risk

- 15.15 Given the nature of the business, there is little likelihood that trade finance will be used by money launderers in the placement stage of money laundering. However, trade finance can be used in the layering and integration stages of money laundering as the enormous volume of trade flows obscure individual transactions and the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements permit the commingling of legitimate and illicit funds.
- 15.16 FATF's June 2006 study of Trade Based Money Laundering²³ defined trade-based money laundering as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail". The study concludes that "trade-based money laundering represents an important channel of criminal activity and, given the growth in world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive". The term 'trade transactions' as used by the FATF is wider than the trade transactions described in this sectoral guidance.
- 15.17 FATF's June 2006 study notes that the basic techniques of trade-based money laundering include:
- **Over Invoicing:** by misrepresenting the price of the goods in the invoice and other documentation (stating it at above the true value) the seller gains excess value as a result of the payment²⁴.
 - **Under invoicing:** by misrepresenting the price of the goods in the invoice and other documentation (stating it at below the true value) the buyer gains excess value when the payment is made.
 - **Multiple invoicing:** by issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one financial institution to facilitate the payments/transactions.
 - **Short shipping:** the seller ships less than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to over invoicing
 - **Over shipping:** the seller ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.

²³ <http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf>

²⁴ A report by Global Financial Integrity showed there was an estimated average of \$725 billion to \$810 billion per annum in illicit financial flows from Developing Countries between 2000 and 2009. Of these amounts, 55% was due to trade mispricing. See <http://iff-update.gfip.org/>

FINAL BOARD APPROVED

- **Deliberate obfuscation of the type of goods:** parties may structure a transaction in a way to avoid alerting any suspicion to financial institutions or to other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety of reasons or purposes.
 - **Phantom Shipping:** no goods are shipped and all documentation is completely falsified.
- 15.18 Generally, these techniques involve fraud by one party against another, but may also depend upon collusion between the seller and buyer, since the intended outcome of the trade is to obtain value in excess of what would be expected from an arms' length transaction, or to move funds from point A to point B without being detected or accounted for by the authorities. The collusion may arise, for example, because the parties are controlled by the same persons, or because the parties are attempting to evade taxes on some part of the transaction.
- 15.19 Some countries require that for the importation of certain types of goods, independent inspection agents certify that the goods meet the specified quality standards and that the prices charged are appropriate. The buyer and seller may also agree to use inspection agents, who will issue a certificate confirming the quality and/or price. Trade Finance staff should understand the circumstances where inspection certificates are required.

Sanctions/proliferation financing

- 15.20 There is at present no agreed definition of proliferation or proliferation financing. FATF's Working Group on Terrorist Financing and Money Laundering has proposed the following definition of proliferation financing for the purposes of its work:

[Proliferation financing is] the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations²⁵.

[Combating Proliferation Financing: A Status Report on Policy Development and Consultation - February 2010]

- 15.21 Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (e.g., certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles).
- 15.22 Dual-use goods destined for proliferation use are difficult to identify, even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised knowledge and experience is often needed to determine if a good may be used for proliferation. Dual-use items can be described in common terms with many uses – such as “pumps” – or in very specific terms with more specific proliferation uses – such as metals with certain characteristics. Further, many goods are only regarded as dual-use if they measure-up to very precise performance specifications.

²⁵ The definition of an *act* of proliferation financing need not involve knowledge. However, when considering the responsibilities of financial institutions or a possible criminal basis of proliferation financing, a subjective element will be indispensable.

FINAL BOARD APPROVED

- 15.23 Proliferation differs from money laundering in several respects. The fact that proliferators may derive funds from both criminal activity and/or legitimately sourced funds means that transactions related to proliferation financing may not exhibit the same characteristics as conventional money laundering. Furthermore, the number of customers or transactions related to proliferation activities is likely to be markedly smaller than those involved in other types of criminal activity such as money-laundering.
- 15.24 There are a variety of United Nations (UN) and national and regional sanctions in place. These include:
- Country-based financial sanctions that target specific individuals and entities
 - Trade-based sanctions, e.g., embargos on the provision of certain goods, services or expertise to certain countries
 - Sectoral sanctions: a comprehensive set of sanctions introduced by the EU and the US aimed at certain industry sectors (financial services, energy, mining and defence) and prohibiting certain types of transactions primarily with a new debt/equity issuance nexus. The applications of such sanctions can be very complex in nature as all aspects of the transaction shall be considered in determination whether it might give rise to a breach. It should be noted, that entities designated within sectoral sanctions regimes are not subject to asset freeze.

In recent years there has also been a series of UN Security Council Resolutions which have, inter alia, introduced targeted financial sanctions and/or activity-based financial prohibitions in respect of certain countries which relate to the prevention of WMD proliferation. For further guidance, firms should refer to the OFSI Guidance on financial sanctions²⁶.

- 15.25 Compliance with the sanctions in force within jurisdictions is relevant to all the products and services offered by firms. Sanctions that require the embargo of certain goods and services have particular relevance in relation to the provision and facilitation of trade finance products.
- 15.26 A summary of the legal and regulatory obligations in relation to proliferation financing is set out in Annex 15-III. Guidance on sanctions screening is given in Part III, section 4: *Compliance with the UK financial sanctions regime*.
- 15.27 The use of trade finance to breach sanctions and/or for the proliferation of weapons of mass destruction (WMD) could potentially take advantage of the complex and fragmented nature of existing global finance activity where multiple parties (in many cases with limited knowledge of one another) become involved in the handling of trade finance.
- 15.28 In June 2008, FATF published a Proliferation Financing Report²⁷ which assessed these risks.
- 15.29 In April 2010 the FATF published a February 2010 report from their Working Group on Terrorist Financing and Money Laundering ‘*Combating Proliferation Financing: A Status Report on Policy Development and Consultation*’ which further analysed the risks and possible policy responses. Annex 15-IV reproduces that report’s discussion of how various types of entity in the financial sector might become involved in proliferation activities.

Assessing the trade-based financial crime risk

- 15.30 A firm's risk-based approach should be designed to ensure that it places an emphasis on

²⁶ <https://www.gov.uk/government/publications/financial-sanctions-faqs>

²⁷ <http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>

FINAL BOARD APPROVED

detering, detecting and disclosing in the areas of greatest perceived vulnerability, in order to counter to the extent practicable the above trade-based money laundering, terrorist financing and proliferation financing techniques.

Annex 15 – VI of this Guidance document provides further information on this for firms.

Money laundering/terrorist financing

- 15.31 The ability of a firm to assess the money laundering/terrorist financing risks posed by a particular transaction will depend on the amount of information that it has about that transaction and the parties to it. This will be determined by the firm's role in the Trade Finance operation. The amount of information available to a firm may vary depending on the size/type of the firm and the volume of business that it is handling. Where possible when assessing risk, firms may take into consideration the parties involved in the transaction and the countries where they are based, as well as the nature of any goods forming the basis of an underlying commercial transaction.
- 15.32 Apart from direct information, firms should have regard to public sources of information that are available at no or minimal direct cost, such as those available on the internet. For example, firms may validate bills of lading by reference to the websites of shipping lines, most of whom offer a free facility to track movements of containers. By using the unique container reference number, firms may be able to confirm that the container was loaded on a designated vessel and that vessel is undertaking the claimed voyage. The websites of many shipping lines provide details of the current and future voyages being undertaken by their ships and up to date information regarding their precise location. Firms would not be expected to investigate commercial transactions outside of their knowledge, although naturally if documentation they see as part of the banking transaction gives rise to suspicion, this should be reported.
- 15.33 When developing a risk-based strategy firms should consider, but not restrict their consideration to, factors such as the size of the transaction, nature of the transaction, geographical location of the parties and the customer's business mix.
- 15.34 Firms need to be aware of trade-based money laundering techniques when developing their risk-based strategy and consider how best to mitigate the risks to themselves. The FATF has listed some red flag indicators in its June 2006 report, which are reproduced in Annex 15-V.
- 15.35 In certain specific, highly structured transactions firms should exercise reasonable judgement and consider whether additional investigation should be undertaken. Such investigation may include determining whether over-invoicing or under-invoicing, or any other misrepresentation of value, may be involved, which cannot usually be based solely on the trade documentation itself. Nor can the use of external data bases alone be relied upon as most products are not traded in public markets and have no publicly available prices. Even where such prices are available, such as those for commodities, firms will not be aware of the terms of trade, discounts involved or quality of the goods etc, so making a determination of the unit pricing will always be difficult. However, where the unit price of goods is materially different from the current market value, firms should consider whether they have a suspicion and whether they should accordingly submit a SAR to the NCA.

Proliferation financing

- 15.36 Particular issues arise in relation to possible proliferation financing risks presented by customers and products, and these are discussed in Annex 15-VI.

General

FINAL BOARD APPROVED

- 15.37 It is recommended that firms create a risk policy (including the risk of financial crime abuse), controls and procedures appropriate to their business which they may be required to justify to their regulators.
- 15.38 Firms should be aware of the addition by the FCA in May 2014 of a new chapter to its *Financial crime: a guide for firms*, in response to the findings from its thematic review of banks' trade finance activities, published in July 2013.
- 15.39 Whilst it is recognised that firms will not be familiar with all types of documentation they see, they should pay particular attention to transactions which their own analysis and risk policy have identified as high risk and be on enquiry for anything unusual.
- 15.40 In addition to this Guidance, firms may also find some useful information in the private sector Wolfsburg Group guidance - Trade Finance Principles 2017 - (see <http://www.wolfsberg-principles.com/> and then go to Wolfsburg Standards – Wolfsburg AML Principles).

*Customer due diligence**General*

- 15.41 With the partial exception of Collections (see below), the required due diligence must be undertaken on the customer who is the instructing party for the purpose of the transaction (see below). Due diligence on other parties to the transaction, including other customers, should be undertaken where required by a firm's risk policy. Reference to Part I, Chapter 5 should be made as appropriate. Additional due diligence on other parties, and possibly on the transaction itself, should be undertaken where required by the firm's internal risk policy and where the firm is specifically on enquiry.
- 15.42 It should be noted that the instructing party will normally be an existing customer of the firm but, if not, due diligence must be undertaken on the instructing party before proceeding with the transaction (see Part I, Chapter 5).
- 15.43 The following list of instructing parties is not exhaustive and where necessary firms will need to decide in each case who the instructing party is (these enquiries are in addition to the standard due diligence undertaken by the firm as a condition of its account relationship):
- Import (Outward) Letters of Credit - the instructing party for the issuing bank is the **applicant**. Questions from the issuing bank that should arise during the initial due diligence process where LC facilities are required would be such as to establish from the applicant:
 - The countries in relation to which the applicant trades, and the trading routes utilised
 - The goods traded
 - The type and nature of parties with whom the applicant does business (e.g., customers, suppliers, etc)
 - The role and location of agents and other third parties used by the applicant in relation to the business (where this information is provided by the applicant).
 - Export (Inward) Letters of Credit - the instructing party for the advising/confirming bank is the **issuing bank**.
 - The advising/confirming bank should undertake appropriate due diligence on the issuing bank (as set out in Part II, Chapter 16: *Correspondent Relationships*). The due

FINAL BOARD APPROVED

diligence may support an ongoing relationship with the issuing bank which will be subject to a relevant risk based review cycle. Due diligence on the issuing bank is not therefore required in relation to each subsequent transaction.

- In other circumstances, the advising bank may not have an ongoing relationship with the issuing bank and may simply act to process the transaction, in which case due diligence may be conducted on a different basis. As a minimum the advising bank will need to ensure that there is a means of authenticating any LC received from the issuing bank.
- Although there is no requirement to carry out customer due diligence on the LC beneficiary, firms may decide to carry out some checks e.g., check existence at Companies House (or equivalent foreign registry), with on-line trade directories, professional advisers or availability of financial statements – subject to their own risk based approach – to confirm the validity of the transaction if the LC is issued by a bank in a country that is considered high risk and if the nature of the transaction (goods, shipment from/to, payment terms etc) warrants further investigation. Financial statements are a useful source of information, as they usually provide a description of the company's main activities, as well as giving information about the size of its financial operations.
- Outward Collections - the instructing party is the **customer/applicant**.
 - Firms should carry out due diligence on the instructing party (exporter) who in many cases will be their customer, on whom they have already carried out due diligence.
- Inward Collections - due diligence should be carried out on the drawee, who will normally be the importer or party acting on behalf of the importer. In most cases the drawee will be an existing customer of the bank receiving the collection, on whom standard due diligence for AML purposes will already have been carried out. Depending on the nature of the transaction and whether it is consistent with the known trading activity of the customer and normal scale thereof, further enquiry may be prudent on a case by case basis.
- Bonds/Guarantees - the instructing party may be either a customer, correspondent bank or other third party.

Sanctions/proliferation financing – CDD and screening

- 15.44 The ability of firms to implement *activity-based controls* against proliferation is limited, due to the lack of technical expertise of firms, the limited information available as a basis for such controls and firms' inability to examine whether such information is correct; the structural differences between money laundering and proliferation financing and the lack of clear financial patterns uniquely associated with proliferation financing; and the fragmented nature of the trade cycle, which limits each firm's visibility of the whole transaction.
- 15.45 *Targeted financial sanctions*²⁸ provide firms with proliferation-related information on which they can take action. Targeted financial sanctions are considered to be most effective when they are implemented globally *i.e.* by the UN, since a designated entity cannot as easily turn to third-country firms to evade sanctions.

²⁸

For the purposes of this guidance, "targeted financial sanctions" includes not only asset freezing, but also prohibitions to prevent funds from being made available to "designated" or "listed" persons and entities.

FINAL BOARD APPROVED

- 15.46 Some jurisdictions have established their own capability to impose targeted financial sanctions on individuals and entities they deem involved in WMD proliferation, independent of sanctions agreed by the UN Security Council. The European Union (EU) has also adopted such sanctions based on specific legislation relating to certain countries of specific proliferation concern.
- 15.47 Targeted financial sanctions may also prompt a proliferation-related entity to conceal its involvement in a transaction. This may involve the use of unusual financial mechanisms which may arouse suspicion among legitimate exporters, or patterns of activity which may generate suspicion of money laundering.
- 15.48 Where lists of entities are available, firms should consider whether undertaking real-time screening of transactions is appropriate. Lists of entities in this context could potentially include both entities subject to targeted financial sanctions e.g., UNSCR 1737, under which transactions with named entities are prohibited; as well as (if such lists are made available), entities of proliferation concern, which have been identified as high-risk by competent authorities and which could be subject to enhanced due diligence and/or suspicious activity reporting. Firms should be careful not unintentionally to treat all types of lists as financial sanctions lists, thus running the risk of prohibiting business with these entities and jurisdictions altogether. Real-time screening against listed entity-names has limitations, however, and may be evaded if the listed entity changes its name or operates through a non-listed front company.
- 15.49 Alternative approaches would be required to identify and prevent proliferation financing activity conducted by non-listed entities. These could include both manual systems – enhanced due diligence, increased monitoring, and enhanced frequency of relationship reviews – and automatic systems such as post-event monitoring of account activity.
- 15.50 Post event monitoring, using multiple risk indicators, may in any event have the potential to identify proliferation financing activity.
- 15.51 *Goods based screening*; evaluation of the goods involved in a transaction very often requires a large amount of technical knowledge only available to export controls experts and/or exporters. Goods lists pose a tremendous challenge even for export control enforcement and certainly a greater one for real time screening than entity lists. Furthermore, firms in general lack the expertise to discriminate between legitimate and proliferation-sensitive goods. Goods lists, in themselves, should not be used as a basis for transaction screening, as their limited effectiveness, and greater difficulty, make them an inefficient safeguard.

CDD and screening section should specify that FIs are expected to perform sanctions screening both at the inception of the trade finance transaction and at the point of submission of the trade finance documents, as some of the transactional details, (e.g. vessels, ports of call etc), may not be known at trade inception and also there could be subsequent updates to the sanctions lists.

Forfaiting

- 15.52 The diverse nature of forfaiting business is such that the exact nature of the transaction needs to be considered. For example, the need to ensure authenticity may lead to enquiries being made of the importer's management, and it may be necessary to examine the commercial parts of documents, dependent on the nature of the underlying commercial transaction.
- 15.53 In the primary Forfaiting, or origination, market, a firm will usually be dealing directly with an exporter, who will be its customer and on whom it should carry out due diligence in accordance with Part I, Chapter 5. In addition, as part of its risk-based approach, a firm, where appropriate, should scrutinise the other party to the underlying commercial transaction, as well as the transaction itself, to satisfy itself of the validity of the transaction. The amount

FINAL BOARD APPROVED

and depth of scrutiny will depend on the firm's risk assessment of the client and transaction.

- 15.54 In the secondary Forfaiting market, the firm's customer will be the person from whom it buys the evidence of debt. However if it holds a Forfait asset to maturity it will be receiving funds from the guarantor bank and thus it should as a matter of course perform due diligence on this entity as well. Using a risk-based approach, firms should also consider whether they should conduct some form of due diligence on the underlying parties to the transaction, as well as on the transaction itself. This will depend on a risk assessment of the countries and the types of clients or products and services involved. It may be necessary to examine documentation on the underlying commercial transaction. However, it should be borne in mind that the further away from the original transaction the purchaser of a Forfait asset is, the harder it will be to undertake meaningful due diligence.

Structured Financing

- 15.55 As stated above, structured finance transactions are diverse in nature. Due diligence should be undertaken on all relevant parties in accordance with the firm's own risk policy/assessment, including, where relevant, certificate of origin to establish the origin of commodities (for example, crude oil)

Enhanced due diligence

- 15.56 Where the nature of a transaction displays higher risk characteristics than normal business undertaken for the customer (instructing party), for example, the buyer falls into a higher risk category then the firm should consider undertaking additional due diligence in line with its risk policies. Some of the checks firms could undertake (not all of which may be applicable or available in each case) include:
- make enquiries as appropriate into the ownership and background of the other parties to the transaction e.g., the beneficiary(ies), agents, shipping lines, taking further steps to verify information or the identity of key individuals as the case demands;
 - seek information from the instructing party about the frequency of trade and the quality of the business relationships existing between the parties to the transaction. This should be documented to assist future due diligence;
 - check the transaction against warning notices from external public sources, for example the ICC's International Maritime Bureau;
 - refer the transaction to external agencies specialising in search and validation services in respect of bills of lading, shipping services and commodity prices, for example the ICC Commercial Crime Services;
 - check details of the source of goods;
 - check public source information for prices of goods such as commodities – where the contract price is significantly different from the market [say 25%] then consider further investigation;
 - attend and record relationship meetings with the instructing party, visit them by arrangement;
 - for export letters of credit, refer details to other Group resources on the ground in the country of origin, to seek corroboration.
 - checks into the verification of shipments after the UCP operation is over, drawn at random from a sample of transactions, across a cross section of the bank's trade finance clients. This may help to identify spurious transactions where buyers and sellers act in collusion.
 - where relevant, certificate of origin to establish the origin of commodities.
- 15.57 The enhanced due diligence should be designed to understand the nature of the transaction, the related trade cycle for the goods involved, the appropriateness of the transaction structure, the

FINAL BOARD APPROVED

legitimacy of the payment flows and what control mechanisms exist.

- 15.58 The nature of business and the anticipated transactions as described and disclosed in the initial due diligence stage may not necessarily suggest a higher risk category but if, during the course of any transaction any high risk factors become apparent, this may warrant additional due diligence. For example – although these may in some cases be used legitimately - where third party middlemen or traders use back to back or transferable LCs to conclude offshore deals, or where the buyer is itself a middleman or trader.

Monitoring

- 15.59 Firms should have regard to the general guidance set out in Part I, section 5.7 on monitoring and in Chapter 6, on reporting suspicious transactions, and requesting consent where appropriate. The depth and frequency of monitoring to be undertaken will be determined by a firm's risk analysis of the business and/or the parties involved. Firms should, however, implement such controls and procedures appropriate to their business, but in any event must comply with any applicable legal or regulatory requirements.
- 15.60 Firms may refer to sources of information that may be relevant to assessing the risk that particular goods may be 'dual-use', or otherwise subject to restrictions on their movement. For example, there are public resources (such as the EC's TARIC database) that can indicate which restrictions might apply to exports from the EU with specific tariff codes: it will show where trade in some types of good under that category might be licensable or prohibited. Exporters must already provide tariff codes to the customs authorities (who use them to calculate the tax levied on the trade), so should be able to provide them to their banks, insurers and their agents. These can be used to identify transactions that might present higher risk or require further due diligence checks, particularly in situations where the risks are perceived to be higher). For example, have issuing banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, been highlighted by national authorities as being of concern? (This information will often be recorded on commercially-available due diligence tools). Does the trade involve jurisdictions previously implicated in proliferation activity?
- 15.61 Techniques dependent on a firm's risk analysis/policy could range from random, after the event, monitoring to checking receivables in any form of securitisation transaction to seek to determine if they are legitimate.
- 15.62 In the automatic monitoring of transactions the drivers that flag 'unusual transactions' tend to be built around:
- payment values
 - volume of payments
 - countries of payment
 - originator/beneficiary names
 - patterns in relation to a country or entity name
 - volume of shipments (e.g., tonnes)

However, the exact configuration of monitoring systems will differ between firms.

- 15.63 Alerts generated from these automatic systems are usually subject to some type of human intervention. Therefore, the effective application of a risk-based approach to monitoring is only possible if based on intelligence-based risk indicators, such as geographical combinations or geographical patterns of high-risk payment flows.
- 15.64 Depending on the screening tool that it employs, a bank may be able to screen SWIFT messages

FINAL BOARD APPROVED

for indications of prohibited or licensed goods, such as armaments.

- 15.65 The ability of a firm to detect suspicious activity will often be constrained. For instance, in the case of fragmented trade finance arrangements the availability of information will be a particularly limiting factor in enabling firm to understand who the ultimate buyer (or seller) of a product is, or what the ultimate end use of product may be. Whilst all firms are expected to have a form of financial transaction monitoring in place, the information presented to a firm will clearly vary according to its role in a particular transaction and the type of payment system used. For instance in the case of letters of credit, the firm will have some – albeit often limited - information on the underlying transaction if it is the issuing bank and less information if it is the advising bank. The extent to which available information will need to be verified will also vary depending on this role.

Staff awareness, training and alertness

- 15.66 The firm must train staff on how trade finance transactions may be used for ML/TF and in the firm's procedures for managing this risk. This training should be directed specifically at those staff directly involved in trade finance transactions, including those in relevant back office functions, and should be tailored around the specific risks that this type of business represents.
- 15.67 Trade Finance staff need to have a high level understanding of export licence regimes and of the importance of seeking evidence from relevant parties to the transaction that an export licence has been obtained for appropriate transactions.
- 15.68 The FATF's red flag indicators set out in Annex 15-V, although directed primarily at governmental agencies, nevertheless should be a useful aid to those devising firms' training programmes. In addition the several case studies set out in the study may also provide good training material.

Glossary of trade finance terms used in this guidance

Bills of Exchange. A signed written unconditional order by which one party (drawer or trade creditor) requires another party (drawee or trade debtor) to pay a specified sum to the drawer or a third party (payee or trade creditor) or order, on demand or at a fixed or determinable future time. In the UK, the relevant legislation is the Bills of Exchange Act 1882, as amended. In cross-border transactions, equivalent laws may also apply. In many other European jurisdictions, transactions will be subject to the Geneva Conventions on Bills of Exchange 1932. Bills of Exchange can be payable at sight or at a future date, and if either accepted and/or avalised, represent a commitment by the accepting or Avalising party to pay funds, thus making them the primary obligor.

Acceptances/Deferred Payment Undertakings. Where the drawee of a bill of exchange signs the bill with or without the word "accepted" on it, the drawee becomes the acceptor and is responsible for payment on maturity. Where banks become the acceptor these are known as "bankers' acceptances" and are sometimes used to effect payment for merchandise sold in import-export transactions. Avalisation that occurs in forfaiting and some other transactions is similar to acceptance but does not have legal standing under English law. Banks may also agree to pay documents presented under a documentary credit payable at a future date that does not include a bill of exchange. In such instances the bank incurs a deferred payment undertaking.

Promissory Notes. These are a written promise committing the issuer to pay the payee or to order, (often a trade creditor) a specified sum either on demand or on a specified date in the future. (This is similar to a bill of exchange).

Guarantees and Indemnities. Sometimes called Bonds, these are issued when a contractual agreement between a buyer and a seller requires some form of financial security in the event that the seller fails to perform under the contract terms, and are normally issued against a backing "Counter Indemnity" in favour of the issuing firm. There are many variations, but a common theme is that these are default instruments which are only triggered in the event of failure to perform under the underlying commercial contract.

Documentary Credits. Historically, these were one of the most commonly used instruments in Trade Finance transactions and although their usage has declined in recent years, particularly in intra-Western European trade, unfavourable credit conditions could reverse this trend, especially in developing markets (at least in the short term). They remain in extensive use in trade involving deep sea transport and in certain geographical areas e.g., South East Asia. In its simplest form a Documentary Credit is normally issued by a bank on behalf of a purchaser of merchandise or a recipient of services (a trade debtor), in favour of a beneficiary, usually the seller of the merchandise or provider of services (a trade creditor). The issuer (usually a bank) irrevocably promises to pay the seller/provider at sight, or at a future date if presented with documents which comply with the terms and conditions of the Documentary Credit. Effectively, the Documentary Credit substitutes the Issuing Bank's credit for that of the applicant subject to the terms and conditions being complied with. When a Documentary Credit is confirmed by another bank, the Confirming Bank adds its own undertaking as principal to that of the Issuing Bank i.e. the Confirming Bank becomes a primary obligor in its own right. There are many more complex variations than this simple example, but almost all Documentary Credits worldwide are issued and handled subject to the applicable International Chamber of Commerce (ICC) Uniform Customs & Practice for Documentary Credits in force (currently UCP 600).

Collections. A typical documentary collection involves documents forwarded by an exporter's bank to an importer's bank to be released in accordance with the accompanying instructions. These instructions could require release of documents against payment or acceptance of a bill of exchange. As with Documentary Credits, there are a number of possible variations and the term collection is also used in

FINAL BOARD APPROVED

other contexts. However, Collections of the type described above are normally but not always handled subject to the applicable ICC Uniform Rules for Collections - URC in force (currently ICC Publication 522).

Standby Letters of Credit. Unlike Documentary Credits, Standby Letters of Credit are default instruments which are sometimes issued instead of a guarantee. They may be issued subject to the applicable ICC rules in force, currently either UCP 600 or International Standby Practices (ISP 98), but may also contain specific exemption wording.

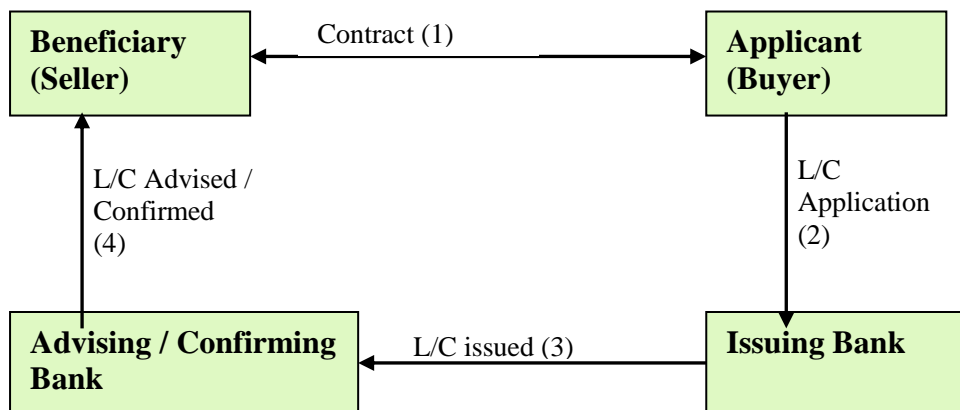
Discounting. A bank may discount a bill of exchange or a deferred payment undertaking, paying less than the face value of the bill/documents to the payee or trade creditor for the privilege of receiving the funds prior to the specified date. The trade debtor may not be informed of the sale and the trade creditor may continue to be responsible for collecting the debt on behalf of the discounter.

Negotiation. This term has a variety of meanings dependent on the jurisdiction/territory in which it is being used but for the purposes of UCP 600 means "the purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) and/or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank".

Forfaiting. This is a financing mechanism traditionally designed for use by trade creditors who export goods. Forfaiting, however, may also involve the direct provision of finance to importers and the provision of working capital by credit institutions for the purposes of funding trade transactions in their countries. The trade creditor or exporter sells evidence of a debt, usually a promissory note issued by the importer or a bill of exchange accepted by the importer or proceeds due under a Letter of Credit such proceeds being assigned by the exporter. The sale is normally made without recourse to the trade creditor/exporter in which case the person buying the debt will usually require the importer's payment obligations to be guaranteed by a bank (avalised).

**The Process for a Confirmed Documentary Credit payable at sight
at the counters of the nominated bank**

Stage 1



Basic Documentary Credit Procedure

The documentary credit procedure involves the step-by-step exchange of documents required by the credit¹⁹ for either cash or a contracted promise to pay at a later time. There are four basic groupings of steps in the procedure: (a) Issuance; (b) Amendment, if any; (c) Utilisation; and (d) Settlement. A simplified example follows:

(a) Issuance

Issuance describes the process of the buyer's applying for and the issuing bank opening a documentary credit and the issuing bank's formal notification of the seller either directly or through an advising bank.

(1) Contract – The Buyer and Seller agree on the terms of sale: (a) specifying a documentary credit as the means of payment, (b) naming an advising bank (usually the Seller's bank), and (c) listing required documents. The naming of an Advising Bank may be done by the buyer or may be chosen by the issuing bank based on its correspondent network.

(2) Issue Credit – The Buyer applies to his bank (Issuing Bank) and the issuing bank opens a documentary credit naming the Seller as beneficiary based on specific terms and conditions that are listed in the credit.

(3) Documentary Credit – The Issuing Bank sends the documentary credit either directly or through an advising bank named in the credit. An advising bank may act as a bank nominated to pay or negotiate (nominated bank) under the credit or act as a confirming bank where it adds its undertaking to the credit in addition to that of the issuing bank. Only in those cases where an advising bank is not nominated to negotiate or confirm the credit is the role of that bank simply an advising bank.

(4) Credit Advice - The advising, nominating or confirming bank informs (advises) the seller of the documentary credit.

(b) Amendment

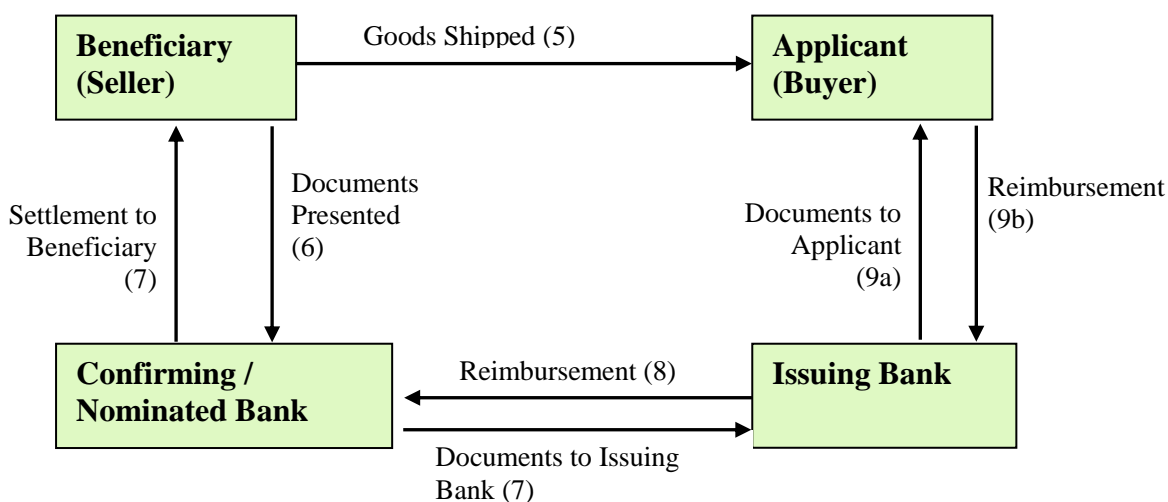
FINAL BOARD APPROVED

Amendment describes the process whereby the terms and conditions of a documentary credit may be modified after the credit has been issued.

When the seller receives the documentary credit, it may disagree with the terms and conditions (*e.g.* the transaction price listed in the credit may be lower than the originally agreed upon price) or may be unable to meet specific requirements of the credit (*e.g.* the time may be too short to effect shipment).

If the seller wants to amend the terms prior to transacting, the seller can request these from the buyer. It is at the discretion of the buyer to adopt the proposed amendments and request an amendment to be issued by the issuing bank. An amended letter of credit would be issued by the issuing bank to the seller through the same channel as the original documentary letter of credit.

Amendments to a letter of credit require the agreement of the issuing bank, confirming bank (if any), and the beneficiary to become effective.

Stage 2***(c) Utilisation***

Utilisation describes the procedure for the seller's shipping of the goods, the transfer of documents from the seller to the buyer through the banks (presentation), and the transfer of the payment from the buyer to the seller through the banks (settlement). For example:

(5) Seller ships goods – The seller (beneficiary) ships the goods to the buyer and obtains the documents required by the letter of credit.

(6) Seller presents documents to Advising or Confirming Bank or directly to the Issuing Bank – The seller prepares and presents a document package to his bank (the advising or confirming bank) consisting of (a) the transport document if required by the credit, and (b) other documents (*e.g.* commercial invoice, insurance document, certificate of origin, inspection certificate, etc.) as required by the documentary credit.

(7) Nominated or Confirming Bank reviews documents and pays Seller – The nominating or confirming bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit and (b) pays the seller (based upon the terms of the credit) which may mean that payment does not occur until after (5). An advising bank does not normally examine the documents, but simply forwards them on to the confirming or issuing bank for their examination.

FINAL BOARD APPROVED

(8) Advising, Nominated or Confirming Bank transfers documents to Issuing Bank – The Advising, Nominated or Confirming bank sends the documentation by mail or courier to the issuing bank.

(9) Issuing Bank reviews documents and reimburses the Nominated or Confirming Bank or makes payment to the beneficiary through the Advising Bank – The Issuing Bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit, under advice to the Buyer that the documents have arrived, and (b) pays the beneficiary through the advising bank or reimburses the nominated or confirming bank (based upon the terms of the credit) and,

(10) Buyer reimburses the Issuing Bank – The Buyer immediately reimburses the amount paid by the issuing bank or is granted a credit by the issuing bank allowing it to reimburse the issuing bank at a later date.

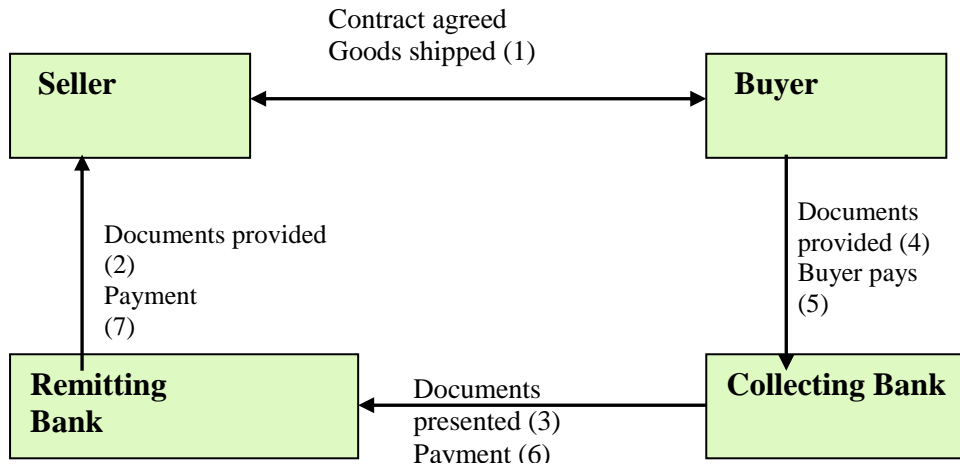
(11) Buyer receives documents and access to goods – The Issuing Bank sends the documents by mail or courier to the buyer who then takes possession of the shipment.

(d) Settlement

The form of payment is specified in the original credit, and must therefore be accepted by the seller. The following are common settlement methods:

- The Sight Credit (Settlement by Payment) – In a sight credit, the value of the credit is available to the exporter as soon as the terms and conditions of the credit have been met (as soon as the prescribed document package has been presented to and checked by the issuing, nominated or confirming bank and found to be conforming to the terms and conditions of the credit) or once the advising bank has received the funds from the issuing bank (unconfirmed). Payment may be affected (sic) directly by the nominated bank or confirming bank upon their examination of the documents and they are reimbursed for that payment by the issuing bank.
- The Usance Credit (Settlement by Acceptance) – In a Usance Credit, the beneficiary presents the required document package to the bank along with a time draft drawn on the issuing, nominated or confirming bank, or a third bank for the value of the credit. Once the documents have been found to be in order, the draft is accepted by the bank upon which it is drawn (the draft is now called an acceptance) and it may be returned to the seller who holds it until maturity.
- The Deferred Payment Credit - In a deferred payment credit the issuing bank and/or the nominated or confirming bank accepts the documents and pays the beneficiary after a set period of time. The issuing, nominated or confirming bank makes the payment at the specified time, when the terms and conditions of the credit have been met.
- Negotiation is the term used where a bank other than the issuing bank agrees to advance funds or discount drafts to the exporter before the issuing bank has paid. Discounting an accepted draft has the same effect.

A letter of credit will normally require the presentation of several documents including a Draft, Commercial Invoice, Transport Document, Insurance Document, Certificates of Origin and Inspection, Packing and Weight Lists.

The Documentary Collection Process

The documentary collection procedure involves the step-by-step exchange of documents giving title to goods for either cash or a contracted promise to pay at a later time.

Contract for the purchase and sale of goods – The Buyer and Seller agree on the terms of sale of goods: (a) specifying a documentary collection as the means of payment, (b) naming a Collecting Bank (usually the buyer's bank), and (c) listing required documents.

(1) Seller ships the goods – The Seller ships the goods to the Buyer and obtains a transport document from the shipping firm/agent. Various types of transport documents (which may or may not be negotiable) are used in international trade and only where required by the underlying transaction is a negotiable document used.

(2) Seller presents documents to Remitting Bank – The Seller prepares and presents a document package to his bank (the Remitting Bank) consisting of: (a) a collection order specifying the terms and conditions under which the bank is to hand over documents to the Buyer and receive payment, and (b) other documents (*e.g.* transport document, insurance document, certificate of origin, inspection certificate, etc.) as required by the buyer.

(3) Remitting Bank sends documents to Collecting Bank – The Remitting Bank sends the documentation package by mail or by courier to the Collecting Bank in the Buyer's country with instructions to present them to the Buyer and collect payment.

(4) The Collecting Bank reviews and provides documents to Buyer – The Collecting Bank (a) reviews the documents making sure they appear to be as described in the collection order, (b) notifies the Buyer about the terms and conditions of the collection order, and (c) releases the documents once the payment or acceptance conditions have been met. Acceptances under documentary collections are known as “Trade Acceptances” which, when accepted (by the Buyer), only carry the obligation of the buyer as opposed to a “Bankers Acceptance” commonly used under a letter of credit which carries the obligation of a bank.

(5) Buyer provides payment to Collecting Bank – The Buyer (a) makes a cash payment, or if the collection order allows, signs an acceptance (promise of the Buyer to pay at a future date) and (b) receives the documents and takes possession of the shipment.

(6) Collecting Bank provides payment to Remitting Bank – The Collecting Bank pays the Remitting Bank either with an immediate payment or, at the maturity date of the accepted bill of exchange if it receives payment from the Buyer.

(7) The Remitting Bank pays the Seller.

ANNEX 15-III

Proliferation financing - the relevant legal and regulatory obligations

1. The system of international and national counter-proliferation controls includes a framework of treaties and United Nations (UN) Resolutions, which ‘universalised’ export controls that were previously implemented mainly on a voluntary and national basis. UN Security Council Resolutions decide also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall; establish, develop, review and maintain controls on providing funds and services related to such export and trans-shipment such as financing.

General obligations: export controls versus financial controls

2. The general obligation on member states is to prevent the activities outlined above. Although UN resolutions primarily require implementation of export controls and do not specifically require states to establish an asset freezing regime, some jurisdictions have implemented national targeted financial sanctions as a route to meet finance-related obligations under the appropriate UN resolutions.
3. Export controls are the primary counter-proliferation safeguard because:
 - International regimes determine the nature of controlled goods - including *dual-use goods*
 - Controlled goods require export licences from national authorities
 - Licences are issued for specific end-users
4. The FATF has studied the specificities and functioning of export controls and the characteristics of international finance. It concluded that financial measures can supplement, but are not a substitute for effective export controls. Export controls are focused on preventing the illegal transfer of proliferation-sensitive goods and may affect financial activity as a secondary effect. Financial measures can reinforce export controls by addressing aspects of an illegal transfer of proliferation-sensitive goods that take place outside the jurisdiction of the country where the illegal export has occurred, such as the financial activities of the associated front company or end-user located in a second jurisdiction.

*Obligations in relation to financial controls**UNSCR*

6. UN Security Council resolutions are addressed to member states, requiring them to take specific actions as regards the subject matter. They therefore do not in themselves directly impose obligations on firms. Member states are required to introduce domestic controls to prevent proliferation and specifically to take actions in relation to sanctioned states.
7. In July 2015 the Joint Comprehensive Plan of Action was agreed between Iran, France, the UK, the US, China and Russia (permanent UN Security Council members), Germany and the EU. In return for Iran curbing its nuclear programme (as attested by the IAEA), the EU, US and the UN agreed to economic and sanctions relief measures. Under the agreement, Iran will eliminate and/or reduce its uranium enrichment activities to avoid proliferation risks and the IAEA will have regular access to all Iranian nuclear facilities.

8. The UN Security Council resolution endorsing JCPOA outlined termination of all previous resolutions targeting Iran's nuclear programme. Under the agreement, US lifted its nuclear related secondary sanctions retaining the primary sanctions, whereby the EU lifted most of its sanctions, including those related to the export of the Iranian oil; however, the arms and ballistic missiles embargo is retained.

(Paragraph 15.29)

WITTING AND UNWITTING ACTORS**[EXTRACT FROM FATF FEBRUARY 2010 WORKING GROUP REPORT]**

Proliferators abuse typical trade structures to facilitate their activities, which include supporters, financiers, logistical support, front companies, assets, shippers and facilitators. Entities that are knowingly engaged in proliferation, such as a front company, may also be involved in legitimate business. Other actors used by a network may knowingly support proliferation, be “wilfully blind” that they are being used for illicit purposes, or are truly unwitting actors. When an entity is engaged in both legitimate and illicit trade it may be less likely for financial institutions to suspect illegal activity.

Front and Other Companies

In individual cases, proliferation networks have employed companies to conceal the true end-use or end-user of traded goods. Most front companies are sensitive to public exposure and disruption of legitimate activities.

Front companies established by proliferators conduct transactions similar to those of companies engaged in legitimate business. Front companies used by proliferators may be similar to those established by money launderers. As is the practice of other criminal organisations, proliferators create companies for a seemingly legitimate commercial purpose and commingle illegal funds with funds generated by legal commercial activity. In some cases, front companies established by proliferators do not engage in any legal activity at all. Front companies may use fraudulent accounting practices and establish various offshore entities in jurisdictions with lax controls to disguise illegal operations. Proliferators are also known to change the names of front companies, or to use multiple names for the same front company, to prevent the detection of the companies’ association with proliferation – or other illicit activity.

Front companies used by proliferators are often located in a major trading hub of a foreign jurisdiction with lax export controls, but may also be found in jurisdictions with more established controls. They can be shell corporations with a fictitious business and physical location or can have normal commercial and industrial operations.

Front companies can arrange shipping services, routing or re-routing goods acquired by the importer or its intermediary. The same and/or additional companies can also be located in jurisdictions with weak financial controls, enabling related financial transactions to settle the underlying trade without detection.

In exceptional cases, front companies may seek complicity within a particular jurisdiction’s government for signoff by national authorities, by production of false cargo manifests to misdirect customs, law enforcement, and intelligence as to the true nature of the goods being exported and their end-use.

Brokers

Brokers are involved in the negotiation or arrangement of transactions that may involve the transfer of items (often between third countries) or who buy, sell or arrange the transfer of such items that are in their ownership. In addition they may also become involved in ancillary activities that facilitate the movement of items such as, but not limited to: *i*) providing insurance; *ii*) marketing; *iii*) financing; and *iv*) transportation / logistics. Illicit brokers illegally participate in proliferation by circumventing existing controls and obfuscating trade activities.

FINAL BOARD APPROVED

Brokers used by proliferation networks are often individuals relying on simple commercial structures, who are very mobile (financially and geographically) so that they can operate from any jurisdiction.

Other Intermediaries

Intermediaries may include companies and individuals that purchase or sell sensitive goods for further manufacture or redistribution. Intermediaries may have a particular knowledge of a jurisdiction's commercial infrastructure. Intermediaries that are knowingly engaged in proliferation will use this knowledge to exploit vulnerabilities in export control systems to the advantage of the proliferator.

Financial Institutions

Proliferation networks may use financial institutions to hold and transfer funds, settle trade and pay for services. Proliferation networks may use both private and public financial institutions for international transactions. States seeking to acquire WMDs may also use foreign branches and subsidiaries of state-owned banks for proliferation finance-related activities, giving these institutions the responsibility of managing funds and making and receiving payments associated with proliferation-related procurement or other transactions. These subsidiaries may be engaged in both legitimate and illegitimate transactions.

ANNEX 15-V

FATF's Trade-Based Money Laundering "Red Flag" Indicators

The respondents to the FATF project team's questionnaire reported a number of red flag indicators that are routinely used to identify trade-based money laundering activities. These include situations in which:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities.
- The type of commodity being shipped is designated as "high risk" for money laundering.*
- The type of commodity being shipped appears inconsistent with the exporter's or importer's regular business activities.
- The shipment does not make economic sense.**
- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason.
- The method of payment appears inconsistent with the risk characteristics of the transaction***
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
- The transaction involves the use of repeatedly amended or frequently extended letters of credit; and
- The transaction involves the use of front (or shell) companies.

[Customs agencies make use of more targeted information that relates to specific exporting, importing or shipping companies. In addition, red flag indicators that are used to detect other methods of money laundering could be useful in identifying potential trade-based money laundering cases.]

* For example, high-value, low volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.

** For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.

*** For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

ANNEX 15-VI

Proliferation financing - Risk assessment of customers and products

1. The purpose of a risk-based approach is not the elimination of risk but rather that firms involved in high risk activity understand the risks they face and have the appropriate policies, procedures and processes in place to manage such risk. Equally, even reasonably applied controls will not identify and detect all instances of proliferation.
2. It would be impractical for firms to be expected to develop a dedicated risk-assessment framework for assessing proliferation financing risks alone. It would be more proportionate to include proliferation considerations alongside the wider determination of risks factors. Moreover, established mechanisms to conduct risk assessment and to identify suspicious activity of wider criminal activity are, in many cases, likely to be applicable to proliferation considerations.
3. The application of a risk-based approach to proliferation financing has both similarities to, and differences from, money laundering. They both require a process for identifying and assessing risk, but the characteristics of proliferation financing – including the limited availability of accessible information to determine risk – result in a more restricted scope for the application of risk-based measures. In acknowledgement of such limitations this guidance seeks to identify potential areas where risk-based decisions could be applied in the area of proliferation financing.
4. Clearly, in some circumstances a risk-based approach will not apply, will be limited, or will be determined by the parameters set by international obligations, national law or regulation. Where particular individuals, organisations or countries are subject to proliferation sanctions, the obligations on firms to comply with certain actions are determined exclusively by national authorities and are therefore not a function of risk. A risk-based approach may, however, be appropriate for the purpose of identifying evasion of sanctions, for example, by directing resources to those areas identified as higher risk.
5. The inclusion of proliferation financing within current risk assessment practices should be proportionate to the overall proliferation risk associated with the activities undertaken by the firm. For example, a firm operating internationally and/or with an international client base will generally be expected to assess a wider range of risks, including proliferation, than a smaller, domestically-focused one.
6. In the application of a risk-based approach, measures and controls implemented by firms may often address more than one identified risk, and it is not necessary that a firm introduce specific controls for each risk. For instance, risks associated with proliferation financing are likely to sit alongside other country, customer and product risks. Additional information that may be useful could include further information on the parties to a transaction, source of funds, beneficial ownership of the counterparty and purpose of the transactions or payment.

Country/geographic risk

7. The most immediate indicator in determining risk will be whether a country is subject to a relevant UN sanction; in these instances some element of mandatory legal obligation will be present, along with risks related to sanctions evasion by sanctioned entities, and proliferation financing by unsanctioned entities. Depending on the extent of risk assessment and business conducted, other factors that may be considered could include:
 - Countries with weak or non-existent export controls (the FATF Proliferation Financing report noted that only 80 jurisdictions have any exports controls related to WMD). Individual

FINAL BOARD APPROVED

country compliance with export control obligations are not, however, currently published. In the absence of such information, firms will not be in a position to make an informed assessment and therefore will not be in a position to utilise this indicator. If, however, such information became forthcoming – either at an international or individual government level – it could provide an additional factor that could potentially inform country risk assessment.

Customer risk

8. Any assessment of the risks that a customer may pose will be underpinned by customer take-on procedures and developed further by ongoing monitoring. Specific categories of customer whose activities may indicate a higher proliferation financing risk could include:
 - Those on national lists concerning high-risk entities.
 - Whether the customer is a military or research body connected with a high-risk jurisdiction of proliferation concern.
 - Whether the customer is involved in the supply, purchase or sale of dual-use and sensitive goods. Firms rely on export control regimes and customs authorities to police the activities of exporters who are their customers. Among others, export control authorities and customs authorities ensure that licensing requirements for dual-use goods have been met. Therefore, the fact that a customer is involved in the supply, purchase or sale of dual-use goods is, of itself, not an indicator for a firm; this would result in a disproportionately large number of trading companies falling into this category. However, a wide range of industrial items and materials can assist WMD programmes and would-be proliferators. The most critical items normally appear on national strategic export control lists, although screening against controlled goods lists is not a practical solution for firms. The involvement in the supply, purchase or sale of dual-use goods may therefore be of some relevance if other risk factors have first been identified.
9. Mitigating factors should also be considered, for example whether the customer is itself aware of proliferation risks and has systems and processes to ensure its compliance with export control obligations.

Transactions risk

10. In determining whether the transaction presents an elevated risk, a number of factors should be considered:
 - Specific nature of the underlying transaction and whether it contains a valid and apparent commercial rationale
 - Terms of the underlying agreement
 - Relationship nature between the FI, client and any potential 3rd party
 - A number of participants involved and consideration of potential fragmentation and complexity
 - Involvement of manual processing/screening of various paper instruments
 - Whether a transaction is conducted on an open account or credit instrument basis

Delivery channels risk

FINAL BOARD APPROVED

11. Customer relationship commenced without a face to face meeting may present a higher financial crime risk than a relationship commenced following a customer meeting. The risks could include:
- Whether the customer legally exists i.e. shell or front company
 - Whether they operate from the stated location
 - Whether the nature of the business activity is as stated
 - Whether the size of the customer is as stated
 - Whether the representatives are the persons who own or control the customer
 - Any other information provided by the customer does not match information which could be obtained by a physical meeting at the place of business

Product and Service Risks

12. Determining the risk of products and services may include a consideration of factors such as:
- Delivery of services to certain entities Project financing of sensitive industries in high-risk jurisdictions.
 - Trade finance services and transactions involving high-risk jurisdictions.
13. As is the case with anti-money laundering, any assessment of risk will need to take account of a number of variables specific to a particular customer or transaction. This will include duration of relationship, purpose of relationship and overall transparency of relationship and/or corporate structure. It would be disproportionate to assess a stable, known customer who has been identified as involved in the supply, purchase or sale of dual-use and sensitive goods as either moderate or high-risk for that reason alone. However, the overall assessment of risk may increase with the presence of other factors i.e., delivering high volumes of dual-use or sensitive goods to a high-risk country/complicated corporate structures/the type and nature of principal parties engaged in the transaction. Consideration of these risks, including customer-specific information, and mitigating factors, will enable a firm to reach a graduated understanding of the degree of proliferation finance risk a particular customer poses.
14. Interpretation of “dual-use” requires a degree of technical knowledge that letter of credit document checkers cannot be expected to possess. In addition, the description of the goods may appear in the documents using a wording which does not allow the identification of such goods as “dual-use”. Regardless of the details in the information sources, however, without the necessary technical qualifications and knowledge across a wide range of products and goods, the ability of a firm to understand the varying applications of dual-use goods will be virtually impossible. It would be impracticable for firms to employ departments of specialists for this purpose.
15. Firms may nevertheless refer to sources of information that may be relevant to assessing the risk that particular goods may be ‘dual-use’, or otherwise subject to restrictions on their movement. For example, there are public resources (such as the EC's TARIC database) that can indicate which restrictions might apply to exports from the EU with specific tariff codes: it will show where trade in some types of good under that category might be licensable or prohibited. Exporters must already provide tariff codes to the customs authorities (who use them to calculate the tax levied on the trade), so should be able to provide them to their banks, insurers and their agents. These can be used to identify transactions that might present higher risk or require further due diligence checks, particularly in situations where the risks are perceived to be higher). For example, have issuing banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, been highlighted by national authorities as being of concern? (This information will often be recorded on commercially-available due diligence tools). Does the trade involve jurisdictions previously implicated in proliferation activity?

FINAL BOARD APPROVED

16. UK exporters seeking to send goods to countries subject to trade restrictions may also be in contact with the Export Control Organisation of the Department for Business Innovation and Skills to clarify whether their shipments will be affected. A firm financing trade with such countries may inquire whether such correspondence has been entered into, particularly if it appears that the goods in question may require an export licence.
17. The Export Control Organisation provides additional guidance at <https://www.gov.uk/guidance/beginners-guide-to-export-controls>. :

16: Correspondent Relationships

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

This sectoral guidance considers specific issues over and above the more general guidance set out in Part I, Chapters 4, 5, and 7, which firms engaged in Correspondent Banking Relationships or Correspondent Trading Relationships should take into account when considering applying a risk-based approach.

Overview of the sector

16.1 Under the ML Regulations, all relationships with Credit and Financial Institutions fall within the definition of Correspondent Relationships. For the purposes of this guidance, however, a distinction is drawn between banking and trading relationships, given the different risks and method of operation. This is reflected in the way that due diligence measures should be applied. Collectively, Correspondent Banking and Correspondent Trading relationships will be referred to as “**Correspondent Relationships**”.

16.2 Correspondent Relationships covers:

- **Correspondent Banking Relationships.** A “**Correspondent Banking Relationship**” is the provision of banking-related services by one bank (**Correspondent**) to another bank (**Respondent**) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network.

Correspondent Banking Relationships can include providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, trade finance arrangements, foreign exchange services, and providing customers of the Respondent with direct access to accounts with the Correspondent (and vice versa). the scope of a relationship and extent of products and services supplied will vary according to the needs of the Respondent, and the Correspondent’s ability and willingness to supply them.

- **Correspondent Trading Relationships.** A “**Correspondent Trading Relationship**” is a relationship among credit institutions or financial institutions for the provision of commercial or business products or services-which may include relationships established for securities transactions or funds transfers, including services within the scope of *Chapter 18 – Wholesale markets* or *Chapter 17 – Syndicated Lending*, or which could simply be the provision of loan finance from one credit or financial services institutions to another. Such relationships may be described as a bilateral commercial arrangement between two institutions, rather than the provision of Correspondent Banking Relationship-related services from one institution to another (as defined above). These relationships do not have a traditional Correspondent and a Respondent since neither party is providing services on behalf of the other or for an underlying customer; accordingly, the degree of ML/TF risk in such relationships is different, generally lower, than it is with relationships which provide for banking-related services on behalf of that institution's customers. They are more similar to normal customer relationships.

FINAL BOARD APPROVED

- 16.3 Generally, in a Correspondent Banking Relationship, a Correspondent is effectively an agent (intermediary) for the Respondent and executes/processes payments or other transactions for customers of the Respondent. The underlying customers may be individuals, corporates or even other financial services firms. Beneficiaries of transactions can be customers of the Correspondent, the Respondent itself or, in many cases, customers of other banks and therefore unknown.

What are the money laundering risks in Correspondent Relationships?

- 16.4 The Correspondent often has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities. Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments (wire transfers – see Part 1, paragraph 5.2.10 - 5.2.13) or clearing cheques.
- 16.5 For these reasons, Correspondent Relationships are, in the main, non face-to-face business and, when an unknown third party is involved, must be regarded as potentially high risk from a money laundering and/or terrorist financing perspective.
- 16.6 Correspondent Banking Relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CTF systems and controls, and customers of those firms, direct access to international banking systems.
- 16.7 A Correspondent handling transactions which represent the proceeds of criminal activity or terrorist financing risks regulatory fines and/or damage to its reputation.
- 16.8 The degree of ML/TF risk presented by different types of Correspondent Relationships between firms will vary, sometimes considerably – for example, some relationships cannot result in payments being made, which clearly carries an almost non-existent degree of risk – and, therefore, the appropriate customer due diligence measures that should be applied will similarly vary, according to the assessed degree of risk.
- 16.9 The primary risk in Correspondent Relationships turns on whether a relationship or transaction is between financial or credit institutions as principal, where the risks are inherently low, especially where the counterparty is based in an assessed low risk jurisdiction. Where the transaction relates to an underlying customer or customers – if this is disclosed, the Correspondent will know who it is dealing with, if undisclosed, this will heighten the risk.

How to assess the elements of risk in Correspondent Banking Relationships

- 16.10 For any Correspondent, the highest risk Respondents are those that:
- deal or trade on behalf of undisclosed customers; or
 - are offshore banks that are limited to conducting business with non-residents or in non-local currency, and are not subject to robust supervision of their AML/CTF controls; or
 - are domiciled in jurisdictions with weak regulatory/AML/CTF controls or other significant reputational risk factors e.g., corruption.
- 16.11 The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken. These risks are particularly relevant for Correspondent Banking Relationships:
- **The Respondent's domicile.** The jurisdiction where the Respondent is based and/or where its ultimate parent is headquartered may present greater risk (or may mitigate the risk,

FINAL BOARD APPROVED

depending on the circumstances). Certain jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Other jurisdictions, however, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments, representing lower risks. Correspondents should review pronouncements from regulatory agencies and international bodies such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the Respondent and/or its parent are based.

- **The Respondent's ownership and management structures.** The location of owners, their corporate legal form and/or a lack of transparency of the ultimate beneficial ownership are indicative of the risk the Respondent presents. Account should be taken of whether the Respondent is publicly or privately owned; if publicly held, whether its shares are traded on a recognised market or exchange in a jurisdiction with a satisfactory regulatory regime, or, if privately owned, the identity of any beneficial owners and controllers. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management turnover. The involvement of PEPs in the management or ownership of certain Respondents may also increase the risk.
- **The Respondent's business and customer base.** The type of business the Respondent engages in, as well as the type of markets it serves, is indicative of the risk the Respondent presents. Involvement in certain business segments that are recognised internationally as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a Respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as activities or countries being especially susceptible of money laundering/terrorist financing or corruption. Equally, a Respondent that has a predominantly low risk customer base, and/or is based in a well-regulated jurisdiction with high AML/CTF standards, carries a lower risk.
- **Downstream Correspondent Clearing.** A Downstream Correspondent Clearer is a Respondent that receives correspondent banking services from a Correspondent and itself provides correspondent banking services to other financial institutions in the same currency as the account it maintains with its Correspondent. When these services are offered to a Respondent that is itself a Downstream Correspondent Clearer, a Correspondent should, on a risk-based approach, take reasonable steps to understand the types and risks of financial institutions to whom the Respondent offers such services, especial care being taken to ensure there are no shell bank customers, and consider the degree to which the Respondent examines the anti-money laundering/terrorist financing controls of those financial institutions.

16.12 Other factors that might affect the Respondent's risk profile include whether:

- the Respondent, their parent or a firm belonging to the same group as the Respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations
- the history of the business relationship with the Respondent gives rise to concern, for example because the amount of transactions are not in line with what the Correspondent would expect based on their knowledge of the nature and size of the Respondent.

16.13 The following factors may indicate lower risk:

- the Respondent is based in an EEA Member State.

FINAL BOARD APPROVED

- The Respondent is based in a third country which has AML/CFT requirements that are consistent with the 2012 FATF Recommendations and effectively implements those requirements.
 - the relationship is limited to a SWIFT RMA plus capability, which is designed to manage communications between financial institutions. This means that the respondent, or counterparty, does not have a payment account relationship.
 - the banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying clients, e.g. foreign exchange services between two banks where the business is transacted on a principal to principal basis and where the settlement of such a transaction does not involve a payment to an unknown third party.
- 16.14 Correspondents must not maintain relationships with Respondents that are shell banks (see Part I, paragraphs 5.3.54 – 5.3.56) nor with any Respondent which provides banking services to shell banks.

How to assess the elements of risk in Correspondent Trading Relationships

- 16.15 The degree of risk in a Correspondent Trading Relationship should be determined bearing in mind the risks inherent in the product and service, and the risks posed by the nature and jurisdictions of operation of the counterparty, in particular whether or not unknown third parties are involved. The risk assessment will essentially follow the firm's standard approach.

Customer due diligence

- 16.16 The customer due diligence measures to be carried out in relation to Correspondent Relationships depends on the particular type of relationship established, where the counterparty is based, and the degree of risk of money laundering or terrorist financing presented by the relationship.
- 16.17 All Correspondent Relationships must be subject to an appropriate level of due diligence which:
- meets the firm's standard customer due diligence requirements, reflecting the degree of risk determined in the relationship, and;
 - ensures that the firm is comfortable conducting business with/for a particular counterparty (and, if applicable, its underlying customers) given the counterparty's risk profile.
- 16.18 For counterparties based in an EEA Member State, the firm will follow its standard customer due diligence procedures, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the firm to apply CDD, SDD or EDD measures in accordance with the guidance in Part I, Chapter 5.
- 16.19 It will be appropriate for a firm to take account of the fact that a counterparty firm is domiciled or operating in a regulatory environment that is recognised internationally as adequate in the fight against money laundering/terrorist financing and corruption. In these instances, a firm may choose to rely on publicly available information obtained either from the counterparty itself, from another reputable existing counterparty, from other credible sources (e.g., regulators, exchanges), or from reputable information sources (e.g. SWIFT KYC Registry), to satisfy its due diligence requirements.
- 16.20 The extent of the Correspondent Relationship should be factored into the level of due diligence undertaken. A firm, under its risk-based approach, may decide to undertake the minimum level

FINAL BOARD APPROVED

of due diligence set out in Regulation 28 for limited correspondent relationships, such as those limited to a SWIFT RMA plus capability, or for Correspondent Trading Relationship transactions undertaken within the UK or the EEA on a bilateral basis.

- 16.21 A firm's policies, controls and procedures should require that the information, including due diligence, held relating to the counterparty to its Correspondent Relationship is periodically reviewed and updated. The frequency of review should be tailored to the assessed degree of risk, and updating should be undertaken as a result of trigger events e.g. an extension to the service/product range provided; a material change to the nature/scope of business undertaken by the Respondent; or as a result of significant changes to its legal constitution, or its owners or controllers or negative regulatory pronouncements and/or press coverage.
- 16.22 In respect of Correspondent Banking Relationships, the level and scope of due diligence undertaken should take account of the relationship between the Respondent and its ultimate parent (if any). In general, for relationships maintained with branches, subsidiaries or affiliates, the status, reputation and controls of the parent entity should be considered in determining the extent of due diligence required on the Respondent. Where the Respondent is located in a high-risk jurisdiction, Correspondents may consider it appropriate to conduct additional due diligence on the Respondent as well as the parent. In instances when the Respondent is an affiliate that is not substantively and effectively controlled by the parent, then the quality of the affiliate's AML/CTF controls should always be established.

The Correspondent, in assessing the level of due diligence to be carried out in respect of a particular Respondent, (in addition to the issues raised in paragraph 16.11) must consider:

- **Regulatory status and history.** The primary regulatory body responsible for overseeing or supervising the Respondent and the quality of that supervision. If circumstances warrant, a Correspondent should also consider publicly available materials to ascertain whether the Respondent has been the subject of any criminal case or adverse regulatory action in the recent past.
 - **AML/CTF controls.** A Correspondent should establish whether the Respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the Respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in the Fourth Money Laundering Directive. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the Respondent's internal policy on money laundering/terrorist financing prevention and its know your customer and activity monitoring controls and procedures. Where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in the Fourth Money Laundering Directive. If not, the extent to which the parent's controls meet FATF standards/equivalent to those laid down in the money laundering directive and whether these are communicated and enforced 'effectively' throughout its network of international offices, should be ascertained.
- 16.23 Correspondent Relationships with shell banks are prohibited in all circumstances and so the firm should satisfy itself that its counterparty is not a shell bank. Firms must also take appropriate measures to ensure that they do not enter into, or continue, a correspondent relationship with a credit institution or financial institution which is known to allow its accounts to be used by a shell bank.

FINAL BOARD APPROVED

- 16.24 Where a counterparty based in a third country is a branch or subsidiary undertaking of a credit or financial institution in an EEA state, the firm should on a risk based approach consider the extent to which EDD measures should be applied. The risk presented by such a customer may be mitigated where they are subject to Group AML/CTF standards that are compliant with the ML Regulations or the EU Fourth Money Laundering Directive and the parent entity is EEA regulated.

Enhanced due diligence for Correspondent Relationships

- 16.25 The ML Regulations prescribe that EDD measures are required to be carried out in respect of Correspondent Relationships with Respondents based in non-EEA jurisdictions. For Respondents based in EEA Member States, the firm's risk assessment will require EDD measures to be applied if the firm determines that the relationship presents a higher degree of ML/TF risk.
- 16.26 Firms need to ensure appropriate EDD requirements are applied to non- EEA counterparties. When considering whether a counterparty should be treated as an EEA institution or a non-EEA institution the relationship should be assessed at the regulated firm level, rather than at the legal entity level. Firms should ensure that they fully document their decision-making process.
- 16.27 Firms should identify whether they are entering into a Correspondent Banking or Correspondent Trading relationship. A Correspondent Banking Relationship is typically higher risk and therefore firms must apply the Enhanced Due Diligence measures in full. By contrast, a Correspondent Trading Relationship, and in particular those where no unknown third party is involved, may be lower risk. In applying EDD measures; however, firms must decide on the precise measures to be applied on a risk sensitive basis.

Enhanced due diligence for Correspondent Banking Relationships

- 16.28 The following EDD measures should be considered for Correspondent Banking Relationships:
- **Nature of Business.** Firms must gather sufficient information about the Respondent to understand fully the nature of its business. The amount of information gathered on the customer may be on a risk based approach and may take into consideration the following (non-exhaustive list):
 - Type of Respondent – an assessment of the credit or financial institution type
 - Business Model – the customer base of the Respondent and the products and services it offers
 - Country of operations – is the Respondent based in a non-EEA country, which has AML/CTF requirements which are equivalent to the ML Regulations and/or the fourth money laundering directive?
 - Does the Respondent have operations in high risk jurisdictions?
 - **Reputation and Supervision.** Firms must determine using credible, publicly available information, the reputation and supervision of the Respondent. Firms should have regard to the following:
 - The disciplinary record of the Respondent – Has the Respondent been subject to recent regulatory enforcement for inadequate AML/CTF systems and controls?
 - Regulated status of the Respondent – Whether the respondent is regulated
 - AML Regime – is the Respondent based in a non-EEA country with an effective AML/ CTF regime?
 - Jurisdiction in which the Respondent is regulated - whether the respondent is subject to adequate AML / CTF Supervision

FINAL BOARD APPROVED

- **Assessment of the Firm's AML / CTF Controls.** Firms must assess the Respondent's AML / CTF framework. This may be applied on a risk based approach, with a varying degree of scrutiny depending on the risks identified as part of the Enhanced Due Diligence process. Firms may also wish to leverage established industry questionnaires or similar to meet this requirement. Additionally, the Correspondent may wish to speak with representatives of the Respondent to obtain comfort that the Respondent's senior management recognise the importance of anti-money laundering/terrorist financing controls.
- **Senior Management Approval.** Firms must obtain senior management approval before establishing a new Correspondent Banking Relationship. The firm should determine who constitutes "senior management" for the purposes of the Correspondent Banking Relationship approval process. However, the approver should have sufficient knowledge of the firm's AML / CTF risk exposure, and of sufficient authority to take decisions affecting the firm's risk exposure. Firms should document internally their approach to customer relationship approvals and should have a sliding scale of approvals depending on the risk of the customer relationship.

A new Correspondent Banking Relationship refers to the initial onboarding of the customer. However, firms should consider, on a risk based approach whether any further senior management approvals might be required by the risk profile of the new product and / or business line being offered and in accordance with the Firms risk assessment of the business.

- **Responsibilities of the Respondent and Correspondent.** Firms must document the responsibilities of the Respondent and Correspondent. In some instances this information may be contained within contractual language (including terms of business) between the Correspondent and Respondent.
- **Direct Access to Correspondent Accounts.** Firms must identify whether the Respondent's customers have access to their accounts. If the Respondent's customers have access, the Correspondent must be satisfied that:
 - The Respondent has verified the identity of, and conducts relevant CDD checks on, their customers on an ongoing basis
 - The Respondent is able to provide upon request the CDD data or information gathered
- **SWIFT (RMA) relationships.** Due diligence should take into account the message types being made available to the respondent bank. Message types Category 1 and Category 2 bring heightened risks and, therefore, enhanced due diligence must be considered in these circumstances.
- **Shell banks.** Whether the Respondent has confirmed that it will not provide banking services to, or engage in business with, shell banks

16.29 The enhanced due diligence process for Correspondent Banking Relationships should involve further consideration of the following elements designed to ensure that the Correspondent has secured a greater level of understanding:

- **Respondent's ownership and management.** For all beneficial owners and controllers, the sources of wealth and background, including their reputation in the market place, as

FINAL BOARD APPROVED

well as recent material ownership changes (e.g. in the last three years), and an understanding of the experience of each member of executive management.

- **PEP involvement.** If a PEP (see Part I, paragraphs 5.5.13-5.5.31) appears to have a material interest or management role in a Respondent then the Correspondent should ensure it has an understanding of that person's role in the Respondent.

Enhanced due diligence for Correspondent Trading Relationships

16.30 In relation to Correspondent Trading Relationships, a firm will apply its standard customer due diligence approach, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the firm to apply CDD, SDD or EDD measures in accordance with the guidance in Part I, Chapter 5.

16.31 Due to the inherently lower risk profile of many Correspondent Trading Relationships, a firm should take the following measures in order to meet the prescribed enhanced due diligence requirements of the ML Regulations relating to Correspondent Trading Relationships with non-EEA based respondents (in addition to its standard customer due diligence approach, based on its determination of the ML/TF risk presented following its risk assessment):

- ensure that the other institution is clearly identified on the firm's records as being the counterparty to the transaction;
- gather information about the nature of the business of the other institution;
- include the institution in the firm's regular customer screening for PEPs, sanctions and other financial crime indicators and follow the same approach as for other customers in terms of assessing and applying the results of such screening within the firm's risk-based approach;
- satisfy itself that the other institution is authorised and regulated in a non-EEA country, which has AML/CTF requirements which are equivalent to the ML Regulations and/or the EU Fourth Money Laundering Directive (and the country receiving an EU or UK equivalence ruling would be sufficient evidence of this), or otherwise undertake an assessment of the other institution's AML/CTF framework. This may be applied on a risk based approach, with a varying degree of scrutiny depending on the risks identified as part of the EDD process. Firms may also wish to leverage established industry questionnaires or similar to meet this requirement, including a determination of the respondent's reputation and the quality of the supervision to which it is subject.
- obtain the approval from senior management before establishing a new Correspondent Trading Relationship. In this regard, the level of seniority of the manager required to make such approval should be commensurate with the risk, provided the approver has sufficient knowledge of the firm's AML / CTF risk exposure, and is of sufficient authority to take decisions affecting the firm's risk exposure. Senior Management should not be taken as meaning persons identified as Senior Managers under the Senior Manager Regime - firms may internally decide who is a "senior manager" for the purposes of approving Correspondent Trading Relationships. For example, relationships with an institution that is authorised and regulated in a non-EEA country which has AML/CTF requirements equivalent to the Fourth Money Laundering Directive (and the country receiving an EU or UK equivalence ruling would be sufficient evidence of this) could be approved by the senior manager of the desk in question.

FINAL BOARD APPROVED

- where appropriate, retain a copy of the terms and conditions which govern the transactions between the firm and the other institution (as the only responsibilities between the two institutions is the performance of the transaction in accordance with its terms); and
- ensure that the other institution is not entering into the Correspondent Trading Relationship on behalf of, or as agent for, a shell bank (in this regard, transaction terms which clearly state that the institution is entering into the transaction as principal and not as agent would be sufficient).

16.32 Where a firm identifies additional risk or is not able to satisfy the measures set out in 16.31, it should consider what further due diligence measures would be appropriate to mitigate the additional risk.

Monitoring of Correspondent Banking Relationships

16.33 Implementing appropriate documented monitoring procedures can help mitigate the money laundering risks for firms undertaking correspondent banking activities. General guidance on monitoring is set out in Part 1, section 5.7.

16.34 The level of monitoring activity undertaken by a Correspondent on its Respondent's activity through it should be commensurate with the risks determined to be posed by the Respondent. Due to the significant volumes that correspondent banking activity can entail, together with the need to work within prescribed scheme settlement deadlines, electronic and/or post-execution monitoring processes are often the norm.

16.35 The following techniques should be considered where relevant for monitoring activity in the area of Correspondent Banking Relationships:

- Anomalies in behaviour
 - Monitoring for sudden and/or significant changes in transaction activity by value or volume.
- Hidden relationships
 - Monitor for activity between accounts, customers (including Respondents and their underlying customers). Identify common beneficiaries and remitters or both amongst apparently unconnected accounts/Respondents. This is commonly known as link analysis.
- High risk geographies and entities
 - Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk geographies and/or entities.
- Other money laundering behaviours
 - Monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds, or transactions in round amounts
- Other considerations

In addition to the monitoring techniques above, the monitoring system employed to monitor correspondent banking for AML/CTF purposes should facilitate the ability to apply different thresholds against customers that are appropriate to their particular risk category.

FINAL BOARD APPROVED

16.36 In addition to monitoring account/transaction activity, a Correspondent should monitor a Respondent for changes in its nature and status. As such, information about the Respondent collected during the customer acceptance and due diligence processes must be:

- Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis), or
- Reviewed on an ad hoc basis as a result of changes to the customers information identified during normal business practices, or
- Reviewed when external factors result in a material change in the risk profile of the customer.

16.37 Where such changes are identified, the Respondent should be subject to a revised risk assessment, and a revision of their risk categorisation, as appropriate. Where, as a result of the review, the risk categorisation is altered (either up or down) a firm should ensure that the due diligence standards for the Respondent's new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

16.38 Firms should consider terminating the accounts of Respondents, and consider their obligation to report suspicious activity, for Respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers featuring in unusual or suspicious transactions or activities.

16.39 The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:

- Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
- Adequacy of staff training and awareness;
- Capturing appropriate management information;
- Upward reporting and accountability; and
- Effectiveness of liaison with regulatory and law enforcement agencies.

Staff awareness, training and alertness in respect of Correspondent Banking Relationships

16.40 Where the firm is a Correspondent, the firm must train staff on how correspondent banking transactions may be used for ML/TF and in the firm's procedures for managing this risk. This training should be directed specifically at those staff directly involved in correspondent banking transactions and dealing with correspondent banking clients and should be tailored around the greater risks that this type of business represents.

16.41 Firms should provide "senior management" approving correspondent relationships with appropriate training to provide them with sufficient knowledge of the firm's money laundering and terrorist financing risk exposure.

Monitoring and staff awareness, training and alertness in respect of Correspondent Trading Relationships

16.42 The monitoring and staff awareness, training and alertness principles set out in Part I of this Guidance would be applicable.

17: Syndicated Lending

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

This sectoral guidance considers specific issues over and above the more general guidance set out in Part 1, Chapters 4, 5, and 7 which firms engaged in syndicated lending may want to take into account when considering applying a risk-based approach.

Overview of the sector

17.1 The syndicated loan market is an organised professional market, international in nature, providing much of the capital used by some of the largest companies in the world for a variety of purposes, ranging from working capital to acquisition financing. Banks and other financial institutions agree to make term loans and revolving credit loans to companies and may syndicate (offer on), or sell off, parts of their commitments to other banks, financial institutions or other entities. (In the case of structured trade finance transactions which may operate on a bilateral or syndicated basis, reference to Part II, Sector 15: *Trade Finance* should be made).

17.2 The following are relationships typically involved in loan syndications:

- **Borrower.** A corporate or other legal entity who seeks to borrow funds and/or arrange credit facilities through the international capital markets.
- **Mandated Lead Manager/Arranger/Bookrunner.** A mandated Lead Manager/Arranger/Bookrunner enters into an agreement to provide credit facilities to a borrower. By the very nature of this appointment, it is likely that the mandated Lead Manager/Arranger/Bookrunner will be a lender with which the Borrower already has an established relationship. A syndicated loan transaction typically may have one to four mandated Lead Managers/Arrangers/Bookrunners and many lenders. The Mandated Lead Manager/Arranger/Bookrunner normally is responsible for advising the Borrower as to the type of facilities it requires, negotiating the broad terms of those facilities and advising on roles, timetable and approach to the market. In some instances it will also underwrite the transaction.
- **Lenders.** The financial institutions that provide the funds that have been arranged for the Borrower by the Mandated Lead Manager/Arranger/Bookrunner.
- **Agent.** To facilitate the process of administering the loan an Agent is appointed. The Agent acts as the agent of the Lenders not of the Borrower, although it is the Borrower that pays the Agent's fees and charges. The Agent acts as an intermediary between the Borrower and the Lenders, undertaking administrative functions, such as preparing documentation, servicing and acting as a channel for information between the Lenders and Borrower. One of the Lenders from the syndicate is normally appointed as the Agent. The Agent has a number of important functions:
 - Point of contact (maintaining contact with the Borrower and representing the views of the syndicate);
 - Monitor (monitoring the compliance of the Borrower with certain terms of the facility);
 - Postman and record-keeper (it is the Agent to whom the Borrower is usually required to give notices); and

FINAL BOARD APPROVED

- Paying agent (the Borrower makes all payments of interest and repayments of principal and any other payments under the loan agreement to the Agent. The Agent passes these monies back to the Lenders to whom they are due. Similarly, the Lenders advance funds to the Borrower through the Agent).
 - When a loan interest is transferred from an existing lender to a new lender, the agent's role is to effect transfers at the request of the outgoing lender by way of execution either of a transfer certificate or an assignment agreement.
 - **Guarantor.** As part of the loan agreement, the Borrower may provide guarantors, who will guarantee repayment of the loan if the Borrower defaults on the loan, on a joint and several basis.
- 17.3 The cash flows arising from these arrangements are between the syndicate participants (lenders) and the Agent, and then on to the Borrower. Similarly, payments made by the Borrower to the Lenders take place via the Agent. The Lenders do not usually have any direct contact with the Borrower in respect of cash flows.
- 17.4 A secondary market also exists where banks and others buy and sell interests in these loans. The treatment of parties within the secondary market is set out in paragraphs 17.16 – 17.23.

What are the money laundering risks in syndicated lending?

- 17.5 Syndicated loans tend to be made to large, often multi-national companies, many of which will have their securities listed, or are parts of corporate groups whose securities are listed, on EU regulated or comparable regulated markets. As such, the money laundering risk relating to syndicated loans for this type of customer should be regarded as low.
- 17.6 The features of all lending are generally that the initial monies advanced are paid into a bank account. In syndicated lending the monies are usually handled by the Agent making it unlikely that the transaction would be used by money launderers in the placement stage of money laundering. Syndicated facilities could, however, be used to layer and integrate criminal proceeds. Repayments are usually made from the Borrower's bank account to the Agent who administers the repayment from its bank accounts to the Lenders. Repayments in cash are unlikely.
- 17.7 Given that a syndicated loan results in the Borrower receiving funds from the Lender, the initial transaction is not very susceptible of money laundering. The main money laundering risk arises through variations in the loan arrangements such as the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination without good commercial rationale. When these circumstances occur they should be considered carefully and consideration must be given to the source of the money used to accelerate the repayment schedule, or terminate the loan early.
- 17.8 The borrower may provide the name of a Guarantor who will repay the loan if the borrower defaults. The main money laundering risk is where the money used by the Guarantor to repay the loan could constitute the proceeds of crime.
- 17.9 The Guarantor may present a sanctions risk at the time of foreclosure. For example, where the Guarantor is located in a sanctioned jurisdiction the lenders may not be able to receive repayment due to sanctions concerns.

Primary market for syndicated loans***Who is the customer for AML purposes?***

FINAL BOARD APPROVED

17.10 The obligation on each party to a syndicated lending arrangement to verify the identity of the customer is as follows:

- **Mandated Lead Manager/Arranger/Bookrunner:** The Borrower is the mandated Lead Manager/Arranger/Bookrunner's customer, as is the Agent.
- **Lenders:** The Borrower is also a customer of the syndicate participants.
- **Agent:** The Agent's customers are the Borrower and the Lenders.

Customer due diligence

- 17.11 The mandated **Lead Manager/Arranger/Bookrunner** should apply the guidance set out in Part I, Chapter 5, and in particular, the guidance on multipartite relationships in Part I, section 5.5, in line with the firm's risk-based approach, to the Borrower and to the Agent.
- 17.12 The **Agent** should apply the guidance set out in Part I, Chapter 5, in line with the firm's risk-based approach, to the Borrower and the Lenders. The Agent, where as part of its risk-based approach it feels it is appropriate to do so, may take account of the due diligence carried out by the mandated Lead Manager/Arranger/Bookrunner on the Borrower. It is often the case that the lenders have pre-existing relationships with the mandated Lead Manager/Arranger/Bookrunner and/or the Agent so that, in practice, little, if any, additional due diligence will need to be undertaken.
- 17.13 The Lender also has a responsibility to apply the guidance set out in Part I, Chapter 5, subject to the firm's risk-based approach, to the Borrower, including where the Lender feels it is appropriate to do so, taking account of the due diligence carried out by the mandated Lead Manager/Arranger/Bookrunner on the Borrower. The Lender should consider their obligations during the lifetime of the lending arrangement.
- 17.14 As the mandated Lead Manager/Arranger/Bookrunner and Agent also have an obligation to verify the identity of the Borrower, the Lender may, where as part of its risk-based approach it feels it is appropriate to do so, take account of the due diligence carried out by the mandated Lead Manager/Arranger/Bookrunner and/or Agent on the borrower where they are in a comparable jurisdiction. In such instances it may be appropriate for the reliance arrangements to be confirmed in a certificate to the Lenders stating that the CDD has been undertaken and documentation is available on request. This may be facilitated by the Borrower undertaking to provide all relevant CDD documentation as set out in Part I, Chapter 5 of this guidance.
- 17.15 The money laundering risk associated with a guarantor only becomes real if a borrower defaults on a loan, and the guarantor is called upon to repay the loan. A firm may consider, subject to its risk-based approach, whether it should verify the identity of the guarantor at the same time as the Borrower, or only to identify the guarantor as and when the guarantor is called upon to fulfil his obligations under the loan agreement. When considering the approach to Guarantors, firms should take into account the nature of the relationship between the Borrower and the guarantor, for example, whether the guarantor is an affiliate/connected party of the Borrower. If the firm decides under its risk based approach only to apply its verification procedures if and when the guarantor is called upon, the firm should still consider applying some degree of identification and screening of the Guarantor at the same time as applying their due diligence procedures to the borrower. Screening of the name at this stage would identify any issues (such as sanctions exposure or parties on an internal watch list) which may become difficult for the firm to avoid following completion of the transaction.
- 17.16 When considering the extent of verification appropriate for a particular borrower, any normal commercial credit analysis and reputational risk assessment and background checks that have

FINAL BOARD APPROVED

been undertaken on the Borrower should be taken into account, and should be factored into a firm's risk-based approach.

Secondary market in syndicated loans

- 17.17 A Lender under a syndicated loan may decide to sell its participation in order to: realise capital; for risk management purposes, for example to re-weight its loan portfolio; meet regulatory capital requirements; or to crystallise a loss. The methods of transfer are usually specified in the Syndicated Loan Agreement.
- 17.18 The most common forms of transfer to enable a Lender to sell its loan commitment are: novation (the most common method used in transfer certificates to loan agreements); legal assignment; equitable assignment; fund participation and risk participation. Novation and legal assignment result in the Lender disposing of its loan commitment, with the new lender assuming a direct contractual relationship with the Borrower, whilst the other methods result in the Lender retaining a contractual relationship with the Borrower and standing between the purchaser in the secondary market and the Borrower. The transfer method should be taken into account by the purchasing firm when considering its customer due diligence requirements.

Customer due diligence

- 17.19 A firm selling its participation in a loan should apply the guidance set out in Part I, Chapter 5, in line with its risk-based approach, when identifying, and if necessary verifying the identity of, the purchaser.
- 17.20 A firm purchasing a participation in a loan should apply the guidance set out in Part I, Chapter 5, in line with its risk-based approach, when identifying, and if necessary verifying the identity of, the seller.
- 17.21 The money flows are typically between the purchaser and seller of the loan. However, if a firm purchases a participation in an existing loan from another participant by way of novation or legal assignment, it will have a direct contractual relationship with the Borrower. As such the purchaser has an obligation to identify, and if appropriate, as part of its risk-based approach verify the identity of the Borrower, in accordance with the guidance set out in Part I, Chapter 5. Where the money laundering risk is low, the Firm may consider the level of Customer Due Diligence required, including, for example, where the loans are being held on a short term basis.
- 17.22 Where a firm purchases a participation in an existing loan from another participant (the Lender) by way of equitable assignment, fund participation or risk participation the seller acts as intermediary between the purchaser and the Borrower for the life of the loan. Depending on the status of the Lender (seller), the purchaser should decide as part of its risk-based approach whether it has an obligation to identify, and verify the identity of, the Borrower, in accordance with the guidance set out in Part I, Chapter 5.
- 17.23 In addition, a firm purchasing a loan in the secondary market must check the underlying Borrower against the Office of Financial Sanctions Implementation's ("OFSI") Consolidated List.
- 17.24 Whether the Agent is required to undertake customer due diligence on a secondary purchaser of a loan participation will depend upon how the transfer between the seller and the purchaser in the secondary market is made:

FINAL BOARD APPROVED

- Where the sale is by way of novation or legal assignment the Agent should, as part of its risk-based approach, identify, and verify the identity of, the purchaser, in accordance with the guidance set out in Part I, Chapter 5.
- Where the sale is by way of equitable assignment, the Agent may not have a direct relationship with the purchaser, even though funds may flow through the Agent from or to the purchaser (via the Lender), and therefore the Agent may not have an obligation to identify and/or verify the purchaser. However, the Agent should consider, as part of its risk-based approach, whether it should identify, or verify the identity of, the purchaser in accordance with the guidance set out in Part I, Chapter 5 and check them against OFSI's Consolidated List.
- Where the sale is by fund participation or risk participation, the Agent will not necessarily be aware of the transaction and therefore has no obligation to identify and/or verify the purchaser or check them against OFSI's.

OUTDATED VERSION

18: Wholesale markets

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

This sectoral guidance considers specific issues over and above the more general guidance set out in Part 1, Chapters 4, 5, and 7, which firms operating in the wholesale markets may want to take into account when considering applying a risk-based approach. Firms may also find the guidance for the following sectors useful:

- Sector 8: *Non-life providers of investment fund products*, which deals with exchange-traded products where the firm acts as agent for private customers, (e.g. where a fund provider that is not an exchange member buys securities for its private customers).
- Sector 9: *Discretionary and advisory investment management*, which covers how investment managers may interact with wholesale markets.
- Sector 10: *Execution-only stockbrokers*, which will be more relevant for firms dealing in wholesale market products as agent or principal for retail customers.
- Sector 14: *Corporate finance*, which deals with the issuance of traded products or instruments, which are traded in a ‘secondary’ wholesale market, allowing investors in the primary market to realise their investment.
- Sector 16: *Correspondent Relationships*, which deals with business relationships between firms.
- Sector 17: *Syndicated lending*, which primarily deals with the syndication of loans and trading on the secondary market.
- Sector 19: *Name Passing Brokers*, which is directed at those firms who deal with wholesale market brokers in the inter-professional markets.
- Sector 20: *Brokerage Services to Funds*, which is intended for firms who are involved in multipartite relationships in respect of, and/or provide services, including the execution and clearing of transaction in wholesale market products to, unregulated funds.

A. Overview of the sector

- 18.1 The wholesale markets comprise exchanges and dealing arrangements that facilitate the trading (buying and selling) of wholesale investment products, and hedging instruments (“traded products”), including, but not limited to:
 - Securities: equities, fixed income, warrants and investment funds (Exchange Traded Funds – ETFs);
 - Money market instruments: FX, interest rate products, term deposits;
 - Financial derivatives: options, futures, swaps and warrants;
 - Commodities: physical commodities and commodity derivatives, including exotic derivatives (e.g., weather derivatives); and
 - Structured products (e.g., equity linked notes).
- 18.2 This guidance provides general guidance on assessing risks in wholesale markets, due diligence and monitoring. It then provides additional guidance on each of the product types referred to above. Reference should be made to both the general and the relevant product-specific guidance in this section, as well as to the general guidance in Part I.
- 18.3 Traded products confer ‘rights’ or ‘obligations’; either between an investor and the issuer, or between parties engaged in the trading of the instruments. Traded products can be bought, sold, borrowed or lent; as such, they facilitate the transfer of property or assets and usually represent

FINAL BOARD APPROVED

an intrinsic value, which may be attractive to money launderers. Traded products can be bought or sold either on an exchange ("exchange traded products"), or between parties 'over-the-counter' ("OTC").

- 18.4 Some traded products or instruments, such as equities, are issued in a 'primary' market, and are traded in a 'secondary' market, allowing investors in the primary market to realise their investment. Other traded products are created to enable investors to manage assets and liabilities, exchange risks and exposure to particular assets, commodities or securities.

Role of the parties

- 18.5 The following are persons typically involved in wholesale market activities:

- **Instructing Counterparty:** The customer on whose behalf the transaction or trade is being conducted;
- **Agent:** An agent in the context of the wholesale markets is an entity which provides related financial services for or on behalf of a customer;
- **Executing Broker:** An executing broker is the broker or dealer that finalises and processes an order to transact/trade on behalf of a customer;
- **Clearing Broker:** A clearing broker settles transactions/trades on behalf of the customer and as such will handle the movement of funds or assets for the customer in settlement of respective transactions and liabilities;
- **Central Counterparty (CCP):** A CCP is an organisation that exists to help facilitate trading activities on certain markets by providing efficiency and stability as a financial intermediary to a transaction/trade;
- **Custodian:** A custodian is a financial institution that holds a customer's securities for safekeeping and protection; and
- **Investment Manager or Adviser:** Funds are managed by an investment manager, which is a separate legal entity from the fund, and which is given authority to act as agent and manage the funds and investments held by the fund vehicle. It is often the investment manager that will make investment decisions and place transactions with a firm as agent of the fund. The investment manager may delegate certain activities to a separate Investment Adviser.

Exchange-traded products

- 18.6 Exchange-traded products are financial products that are traded on exchanges, which have standardised terms (e.g. amounts, delivery dates and terms) and settlement procedures and transparent pricing. Firms may deal in exchange-traded products as principal or as agent for their customers. In the financial and commodity derivatives markets, firms will typically deal as principal, and on certain exchanges (e.g. Euronext.LIFFE, ICE Futures, LME) must do so when dealing as a clearing member in relation to their customers' transactions. In the securities markets, firms can deal as either principal or as agent for the firms' underlying customers.
- 18.7 The London Stock Exchange recognises different types of relationships between a settlement agent and its customers, which it denotes as Model A and Model B. Similar relationships may be recognised on other exchanges and different terminology used to denote these relationships.
- 18.8 Most exchanges have a CCP which stands between the exchange members that are buying and selling a product (becoming the buyer to the seller and the seller to the buyer). Where an exchange or trading platform does not have a CCP, the members contract with each other.

FINAL BOARD APPROVED

OTC products

- 18.9 OTC products are bilateral agreements between two parties (or may be multilateral agreements, depending on the settlement process), that are not traded or executed on an exchange. The terms of the agreement are tailored to meet the needs of the parties, i.e., there are not necessarily standardised terms, contract sizes or delivery dates. Where firms deal OTC, they usually deal as principal. Some OTC dealing is facilitated by brokers and, while settlement is normally effected directly between the parties, it is becoming increasingly common for exchanges and clearers to provide clearing facilities (i.e., the trades are executed as OTC but are then given up for clearing by a CCP).

B. What are the money laundering risks in the wholesale markets sector?

- 18.10 Traded products are usually traded on regulated markets, or between regulated parties, or with regulated parties involved acting as agent or principal.
- 18.11 However, the characteristics of traded products, which facilitate the rapid and sometimes opaque transfer of ownership, and the ability to change the nature of an asset and market mechanisms that potentially complicate the audit trail, together with a diverse international customer base, present specific money laundering risks that need to be addressed and managed appropriately. *[Note: the "National risk assessment of money laundering and terrorist financing 2017" has been taken into account when updating this chapter and this guidance is considered to accord with the provisions of that document.]*
- 18.12 Given wholesale markets' global flows of funds, speed of transactions and potential ease of converting holdings to cash, they are capable of being used for money laundering, but it is important to recognise that these markets may be abused by criminals at different stages of the money laundering process and that the risks of money laundering in the wholesale markets may vary, depending upon the products and services a firm offers to a customer. It is important for a firm to understand at which stage(s) risks may arise (and this may vary from firm to firm):
- Placement: It is unlikely that physical currency or bearer instruments could be placed into the wholesale financial markets, as the primary acceptance of such assets is not a service offered by firms carrying out business in the UK within this sector.
 - Layering: The wholesale financial markets grant the means to execute and clear a chain of transactions which may be complex, involving a multitude of financial instruments and/or financial institutions. This environment may potentially be abused by a criminal to layer funds and/or asset ownership with an aim of obfuscating the illicit origin of such funds/assets. Methods such as 'mirror trading', 'wash trading' or 'offsetting transactions' have been identified by the FCA as having been utilised in a manner highly suggestive of financial crime²⁹. A firm should also consider whether it facilitates the electronic transfer of funds into the wholesale market sector from an outside source, particularly from a third party or jurisdiction considered to present a higher risk for money laundering.
 - Integration: Some financial instruments transacted on the wholesale markets can be rapidly liquidated to cash or reinvested into other holdings. A firm may then facilitate the further integration of these funds through the purchase or transfer of other existing assets. Whilst these activities are generally legal and legitimate, firms should consider the associated and varied money laundering risks when a customer instructs the transfer of value (by payment or change of asset ownership) to an overseas jurisdiction, particularly where a third party is involved.
 - Post-integration (use of criminal proceeds): It can be very difficult to identify proceeds of crime once they have been integrated and mixed with legitimate funds in wholesale market products. Once proceeds of crime have been integrated in this way, it is likely that only the firm whose customer is the end party (and which would therefore have carried out customer

²⁹ <https://www.fca.org.uk/publication/final-notice/deutsche-bank-2017.pdf>

FINAL BOARD APPROVED

due diligence ("CDD") on that party) would be in a position to potentially identify such proceeds, by identifying any irregularity/inconsistency between the value of the transaction and its customer's source of wealth or funds (although such inconsistencies may, even then, be difficult to identify). Where the end party already has significant legitimate wealth, the use by that party of the proceeds of crime for investment purposes (rather than further layering of funds) will, again, be difficult to identify, even by the firm which has conducted CDD on that party as its customer.

- 18.13 Firms dealing in traded products in the wholesale markets do not generally accept cash deposits or provide personal accounts that facilitate money transmission and/or third party funding that is not related to specific underlying investment transactions. Third party payments may, however, be used in relation to particular products, such as FX and/or commodities. Firms should consider whether third party payments are possible and whether the ability to make such payments presents additional money laundering risks, and should have regard to the product-specific guidance in this chapter where relevant.
- 18.14 The extent to which certain products are subject to margin or option premium payment arrangements will affect the level of risk. The nature and form of any margin will need to be taken into account by the firm, through its risk-based approach, when identifying the customer and determining appropriate payment procedures.
- 18.15 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in assessed lower risk jurisdictions, are transparent and have a CCP to clear trades, can ordinarily be seen as carrying a lower generic money laundering risk. OTC business will, generally, be less transparent, and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. For example, exchanges often impose specific requirements on position transfers, which have the effect of reducing the level of money laundering risk. These procedures will not apply in the OTC markets, where firms will need to consider the approach they would adopt in relation to any such requests in respect of customers dealing OTC. Trades that are executed as OTC but then are centrally cleared may have a different risk profile to trades that are executed and settled OTC. Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

C. How to assess the elements of risk in the wholesale markets sector

- 18.16 The main factors to consider when assessing the risk when undertaking business in the wholesale markets are: the nature of the customer; the market participants; the products involved; and whether the products are exchange traded or OTC.
- 18.17 When implementing a risk-based approach, producing or reviewing risk assessments, or assessing the risk profile of a prospective customer, there are a number of areas which firms may want to take into account in addition to the more general matters set out in Part I, Chapters 4 and 5.
 - The wholesale markets are populated by customers with a wide range of different business interests. The types of participants present might typically include, but are not limited to:
 - Sovereign governments;
 - Local authorities (municipal bodies);
 - Regulated financial firms (e.g. banks, brokers, investment managers and funds);
 - Unregulated financial entities (e.g. off-shore funds);
 - Corporations (e.g. listed companies, private companies); or
 - Trust and partnerships.

FINAL BOARD APPROVED

- A customer's nature, status, and the degree of independent oversight to which it is subject may affect the firm's assessment of risk for the particular customer or for the firm's business as a whole.
 - The instruments traded in the wholesale markets can allow for long-term investment, speculative trading, hedging and physical delivery of certain financial instruments and commodities. Understanding the role of a prospective customer in the market, and the customer's reasons for trading, will help inform decisions on the risk profile the customer presents.
 - The way that a firm addresses the jurisdictional risk posed by a customer will depend on a number of factors. Jurisdictional risk should be considered but may, in relevant cases, be mitigated by the rationale for the customer being located or operating in a particular jurisdiction; customers located in potentially higher risk jurisdictions may have legitimate commercial interests which can mitigate the perceived risk, and presence in a higher risk jurisdiction does not necessarily render a customer high risk for AML/CTF purposes. For example, an oil producer in a higher risk territory may seek to use derivative instruments to hedge price risks and this does not necessarily present a high money laundering risk.
 - Firms should ensure that any factors mitigating the jurisdictional or other risks of a customer are adequately documented and periodically reviewed in the light of international findings or developments, and due diligence gathered as part of ongoing monitoring.
 - Firms should take a holistic view of the risk associated with a given situation and note that the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.
 - For discussion of other risk areas firms may need to take into account, such as corruption risk, see paragraph 18.20.
- 18.18 When dealing on an exchange or trading platform, a firm needs to identify its counterparty (section D below describes who should be subject to CDD) and consider any associated risks:
- Where there is a CCP, a firm must assess the risks associated with the exchange. For example, what value can be placed on the exchange's admission procedure, does the exchange carry out due diligence on potential members, can private individuals be members?
 - If there is no CCP, a firm will need to perform due diligence on the party with whom it deals - even if their name is not known until after the trade - before the trade is settled.
 - As a result of trading on an exchange or trading platform, a firm may execute a trade with a member who does not have an account with the firm. A firm should consider obtaining, from the exchange or trading platform, a list of members and either identify and verify them upfront (to avoid possible delays in settlement) or on a case by case basis. In some cases platforms operators provide credit management functionality which has the effect of restricting execution of trades to certain counterparties only.
- 18.19 Product risk should also be considered. Transactions which give rise to cash movements (such as those associated with structured products) may present an increased money laundering risk, although this risk may be mitigated by the nature and status of the customer and the depth of the relationship the customer has with the firm. For example, if the use of a particular product is part of a wider business relationship, and is compatible with other activity between the firm and the customer, the risk may be reduced.
- 18.20 While assessing ML/TF risks, firms will also wish to assess other factors such as reputational risk, sanctions risks and bribery and corruption risks. For example:
- New customers and payments on behalf of clients to third parties will typically need to be screened for sanctions purposes, and new additions to sanctions lists checked against existing clients, in line with the firm's approach to sanctions compliance.

FINAL BOARD APPROVED

- Firms should assess whether they have a due diligence requirement in respect of any introducing brokers who introduce new customers or other intermediaries and consider whether there are any red flags in relation to corruption risks.

D. Customer due diligence, including simplified and enhanced due diligence*Who is the customer?*

- 18.21 It is important to distinguish the relationships that exist between the various parties associated with a transaction. In particular, the firm should be clear whether it is acting as principal, or agent on behalf of the customer, and whether the firm has a responsibility, on a risk-based approach, to verify the identity of any underlying customers of parties involved in transactions.
- 18.22 Where the firm's customer qualifies for simplified due diligence (see Part I, section 5.4), or is otherwise assessed as posing a lower risk, a lesser extent of CDD may be appropriate (as described by Chapter 5).
- 18.23 Therefore, from an AML/CTF perspective, as a rule of thumb (although see Part I, Chapter 5, section 5.3.4):
- If the firm is acting as principal with another exchange member, the exchange member is the firm's customer.
 - As discussed in paragraph 18.18 above, where an exchange-based trade is randomly and automatically matched with an equal and opposite exchange-based trade, it is recognised that, due to market mechanisms, the name of the other exchange member(s) may not be known. In these situations, where all the parties are members of the exchange and there is a CCP to match and settle the trades, the firm cannot know and therefore does not need to identify the other exchange member. Firms should, however, include the money laundering risk involved in the participation in any exchange or centralised clearing, as part of their overall risk-based approach. Participation in any exchange or centralised clearing system does not remove the need to adequately verify its own customer if the firm is dealing as agent for a customer.
 - Where a firm is acting as principal with a non-exchange member, the non-exchange member is the firm's customer.
 - Where a firm executes a trade OTC with a customer, which is then centrally cleared, and settled by the CCP, the firm has visibility of the customer and may need to verify the identity of the customer with whom they contract. By contrast, the CCP would not be a customer of the firm, and as such the firm would not be required to conduct due diligence on the CCP from an AML/CTF perspective. In certain situations, the firm may open customer accounts at the request of a CCP, in which case due diligence obligations would arise. However, this would only occur in a default management scenario, and such arrangements would be documented in a separate customer agreement with the CCP.
 - Where a firm is acting as agent for another party, the party for whom the firm is acting will be the firm's customer.
 - Where the firm is transacting with a counterparty trading as agent for underlying entities, the counterparty will be the customer of the firm provided simplified due diligence can be applied, or provided that the counterparty is otherwise assessed as posing a lower risk. See Part I, Chapter 5, section 5.6.36ff, which considers whether/when underlying entities will also be customers of the firm.
- 18.24 Where the firm is performing services on behalf of an investment manager, the investment manager is the firm's customer. An investment manager may itself be acting on behalf of an underlying entity, such as a fund, to whom it may provide advisory or discretionary investment management services. Whether CDD is performed on the underlying entity will depend on the firm's business relationship with both entities and the nature and status of the investment

FINAL BOARD APPROVED

manager. As stated in Part I, Chapter 5, paragraph 5.6.38, where a firm takes instruction from an underlying entity, or where the firm acts on the underlying entity's behalf (e.g., as a custodian), the firm then has an obligation to carry out CDD measures in respect of that entity.

18.25 Accordingly, when determining whether CDD should be performed on the underlying entity, firms may wish to undertake a risk assessment that includes consideration of whether:

- (i) the investment manager or the underlying entity is the instructing party (e.g. does the investment adviser/manager have discretionary trading authority and full control to instruct transactions);
- (ii) the investment manager is incorporated in a jurisdiction assessed, by the firm, as lower risk;
- (iii) the investment manager is subject to and supervised for compliance with satisfactory anti-money laundering requirements, for example because it is subject to national legislation implementing the EU Fourth Money Laundering Directive; and/or
- (iv) the product or service is assessed, by the firm, as lower risk (see 18.19 above).

18.26 In circumstances where the firm determines that CDD should be performed on the underlying entity, the firm may consider reliance subject to provisions of Regulation 39 of the ML Regulations (see Part I, Chapter 5, section 5.6.4 – 5.6.23), with regards to CDD on the underlying entity.

18.27 Where a firm is receiving services from a counter-party broker, the firm is the customer of the counter-party broker and it is not required to conduct CDD on that broker (although it may decide, on a risk based approach, that some form of due diligence is appropriate).

Other multi-partite relationships

18.28 An introducing broker may “introduce”, or a Receiver and Transmitter of orders may pass orders from, his customers to a firm to execute trades and, possibly, to perform related requirements in connection with the customers’ trades and bookkeeping and record keeping functions. A fee is paid by the firm to the introducing broker, usually based on the transactions undertaken. A customer often has no say in which firm the introducing broker selects to execute a particular trade. As such, the customer being introduced is a customer of both the introducing broker and the firm. Although an introducing broker may not be considered the firm's customer, a firm may wish to consider whether it should carry out due diligence, in particular in light of the "corporate offences" contained in the Bribery Act 2010³⁰ and/or the Criminal Finances Act 2017³¹, as the introducing broker may be considered an "associated person".

18.29 A non-clearing member of an exchange may maintain one or several accounts with a clearing member. Where a non-clearing member deals as agent for a customer, this may be through an omnibus account with the clearing member on behalf of all the non-clearing member’s underlying customers, who often have no say in the non-clearing member’s selection of a clearing member.

- Where a non-clearing member deals on a proprietary basis as principal, it will generally operate a separate account for such business. In that case the non-clearing member will be the customer of the clearing member.
- The clearing member may, based upon his risk-based approach and/or the status of the non-clearing member, consider that the non-clearing member’s underlying customer or customers are also his customers. For further guidance refer to Part I, sections 5.3 and 5.4.

18.30 Customers wishing to execute and clear transactions on regulated markets may do so using separate executing and clearing brokers. To complete such a trade, the executing broker will

³⁰ <http://www.legislation.gov.uk/ukpga/2010/23/contents>

³¹ <http://www.legislation.gov.uk/ukpga/2017/22/contents>

FINAL BOARD APPROVED

execute the order and then ‘give-up’ that transaction to the clearing broker for it to be cleared through the relevant exchange or clearing house.

- 18.31 This arrangement may commonly take the form of a tri-partite agreement between the customer, the executing broker and the clearing broker. However, give-up arrangements can extend to cover a number of different types of relationships.
- 18.32 As set out in paragraph 18.63 of this chapter, where a firm acts as executing broker, the party placing the order is the customer for AML/CTF purposes.
- 18.33 Where a firm acts as clearing broker, the customer on whose behalf the transaction is cleared is the customer for AML/CTF purposes. A clearing broker typically has a more extensive relationship with the customer as they may also act as custodian.
- 18.34 Where an executing broker and a clearing broker are involved in a ‘give up’ arrangement, the executing broker may, as part of its risk-based assessment, consider it appropriate to place reliance on the clearing broker (subject to the guidance and requirements within Part I, Chapter 5, paragraphs 5.6.4ff).
- 18.35 In some cases, other parties, who are not customers under the ML Regulations, may be linked to a transaction. A firm may, however, still wish to assess them as part of its own commercial due diligence and to guard against reputation, sanctions and bribery and corruption risks (e.g., introducing brokers, particularly in higher risk jurisdictions, for the reasons described above).

Distributors

- 18.36 Firms who use third party distributors to distribute, sell and/or market particular products will generally have a customer relationship with the distributor, rather than the underlying entity (who is the customer of the distributor).
- 18.37 Firms should carry out CDD on the distributor in accordance with the provisions of Part I and will wish to consider seeking information and/or assurances about the distributor's own AML procedures (and the procedures the distributor has in place to mitigate other financial crime risks). The firm can also seek contractual protections in the distribution agreement.

Introducers of structured products contracting via custodians

- 18.38 In one scenario, an introducer (who may also be described as an “arranger” or “retrocession agent”) may approach a firm to request, on behalf of an undisclosed client, a quote for a structured product with a particular set of features (e.g., reference assets/indices, capital guarantee, maximum upside, etc). If this quote is acceptable, the introducer will then recommend the structured product to his/her client. The introducer’s client will typically contact their custodian bank to instruct the bank to purchase the structured product from the firm. The custodian bank will purchase, on an execution-only basis, the structured product as principal, settling directly with the firm. The firm then pays the introducer a fee, which is non-standardised and negotiated on a transaction by transaction basis. Alternatively, the firm may approach the introducer with a structured product that the introducer’s clients may be interested in (although transaction flows remain the same as above).
- 18.39 In some cases, the introducer may act with a power of attorney from their client and thus have authority to purchase the structured product on behalf of the client. The firm should ascertain whether the introducer is acting under a power of attorney or not. Settlement of the transaction will be effected, by the firm, with the custodian bank of the undisclosed client, as outlined above.
- 18.40 Depending on local legislation, an introducer may or may not be required to be regulated in the country of his domicile or the countries of his/her main operation, which may be different. In Switzerland, for example, introducers who act exclusively in an advisory capacity do not need to be regulated but where the client gives an introducer power of attorney to transact on his behalf with the custodian bank, the introducer has to be regulated for AML purposes, but not conduct of business purposes, with one of the local Self Regulatory Organisations.

FINAL BOARD APPROVED

- 18.41 In each of the scenarios outlined above, the introducer should be subject to CDD. As part of that CDD, a firm should check that the introducer satisfies the authorisation requirements (if any) of the introducer's country of domicile and main countries of operation. The firm should also consider obtaining details of the career in the financial services industry of each of the main employees or principals of the introducer.

In addition, if the custodian bank cannot be subject to simplified due diligence or is not otherwise regarded as posing a lower risk, the firm will also have to look through to the custodian's underlying customers (the beneficial owners). Firms may also wish to refer to the 'Retail Structured Products: Principles for managing the provider-distributor relationship' guidance, that was published in July 2007 by the European Securitisation Forum (ESF), International Capital Market Association (ICMA), International Swaps and Derivatives Association (ISDA) and the Association for Financial Markets in Europe (AFME). A copy of this guidance is available from the website of any of the above organisations. Firms may also wish to refer to this guidance to assist them in understanding the types of underlying entities that are linked to an individual introducer, together with the particular type of products and tenor of the products that the underlying entities are interested in. Such information may assist firms to understand the expected type and level of business that an introducer may bring to a firm.

- 18.42 Firms should consider, if an introducer requests that his fee be paid to a bank account held in the name of an apparently unrelated third party or to an account at a bank in a country with no obvious connection to his country of domicile or his countries of main operation, whether such requests give rise to suspicions of bribery, corruption or tax evasion. Firms may wish to consider introducing a policy of paying fees only to a bank account in the name of the introducer that is held at a bank in the country of the introducer's domicile or a country of main operation. Firms may also wish to confirm that there is full disclosure of any fees on relevant documentation for each transaction.
- 18.43 Firms should also be alert to the risk that an introducer who is an individual may be carrying on their own personal business whilst still employed by, and managing the affairs of clients of, another firm such as a bank, asset manager or wealth manager. The introducer may be acting in his/her own name or via a corporate which he/she controls. If, as a result of its CDD, a firm has suspicions that an introducer may be currently employed by a financial institution, the firm should contact the financial institution concerned to ascertain whether the individual is employed by them and, if so, that they are content with the proposed relationship between the firm and their employee. Similar suspicions may also arise where all of an introducer's clients use the same custodian bank.

Expected activity

- 18.44 A firm will, as part of CDD, assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship and/or transaction. This information will assist firms when assessing whether the proposed relationship is in line with expectations and will support ongoing monitoring. The key consideration is being able to identify whether the client's activity (for example: transaction size and frequency) is in line with the firm's knowledge of the client. The firm will, in many cases, be able to infer the client's expected activity from the nature of the client itself (e.g. regulated financial institutions can generally be expected to trade products consistent with the typical operating model of such an institution).
- 18.45 Clients will typically have multiple brokers and deal in a multitude of products and asset classes and their strategy may be dependent on market conditions, which may influence changes in activity.

Source of wealth

- 18.46 A firm should, where appropriate, identify the source of wealth relevant to the business relationship and/or transaction. In the wholesale markets, the source of wealth for a counterparty may often be identifiable from the nature of the customer's business. Firms may

FINAL BOARD APPROVED

wish to infer source of wealth where the relationship is deemed to be lower risk. However, where the relationship is with an entity which is indicative of personal wealth of an individual or a collective group of individuals (e.g. family offices), a firm may take additional steps to identify and verify, where appropriate, the client's source of wealth (see also Part II, Chapter 5 on wealth management). Additionally, if settlement or collateral posting is received from a third party, firms should consider the rationale for this.

Source of funds

18.47 The source of funds may be identified and verified in certain situations to ensure the origin of the funds involved in the business relationship or occasional transaction is understood. Whether the identification and verification of a customer's source of funds is required will depend on the nature and status of the entity wishing to execute and clear wholesale markets transactions. If the entity is within points (i) and (ii) below (i.e. having an appropriately regulated and supervised status), or is otherwise determined to present a low ML/TF risk, the firm may, on a risk-based approach, conclude that it is not necessary to obtain specific evidence of the source of funds:

- (i) subject to requirements in national legislation implementing the EU Fourth Money Laundering Directive (or equivalent) as an obliged entity (within the meaning of that Directive); and
- (ii) supervised for compliance with those requirements in accordance with Chapter VI of the EU Fourth Money Laundering Directive (or equivalent).

18.48 In situations where the customer takes the form of a privately-controlled, unregulated entity (including, in particular a private investment company, SPV or family office) the risk is likely to be assessed as higher, and in cases which present a higher ML/TF risk, the source of funds for a business relationship or occasional transaction should be identified and, on a risk-based approach, verified by a firm in order for the firm to reasonably satisfy itself that the origin of the funds is legitimate.

Simplified due diligence

18.49 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 and the matters specified in Regulation 37 of the ML Regulations, the business relationship or transaction presents a low degree of risk of ML/TF.

18.50 In the wholesale markets, a firm will often interact with other regulated firms, some of whom may be acting on behalf of underlying entities. In this context, firms should have regard to paragraphs 18.23 to 18.27 of this Chapter.

Enhanced due diligence (including Correspondent Relationships)

18.51 The ML Regulations prescribe that EDD measures are required to be carried out in respect of Correspondent Relationships with Respondents based in non-EEA jurisdictions (see Part II, Chapter 16 for the definition of a "Correspondent Relationship").

- For respondents based in EEA member states, the firm's risk assessment will require EDD measures to be applied if the firm determines that the relationship presents a higher degree of ML/TF risk.
- In meeting the prescribed EDD measures for non-EEA counterparties, a firm should consider the matters set out in paragraphs 16.26-16.32 and should document its decision-making process.

18.52 Otherwise, product risk alone will not ordinarily be the determining factor in a firm assessing whether an enhanced level of due diligence is appropriate; therefore there are no enhanced due diligence requirements specific to the wholesale markets sector, over and above those set out in Part I, section 5.5, which take into account other risk factors such as client type and jurisdictional risk.

E. Monitoring and surveillance

- 18.53 Guidance on general monitoring requirements is set out in Part I, section 5.7.
- 18.54 Monitoring in wholesale firms will be affected by the fact that firms may only have access to a part of the overall picture of their customer's trading activities. The fact that many customers spread their activities over a number of financial firms will mean that many firms will have a limited view of the entirety of a customer's trading activities. Extreme market conditions may also impact on a customer's trading strategy and the commercial rationale for a particular transaction will often be linked to market conditions. There are, however, specific characteristics of the wholesale market sector which will impact a firm involved in the wholesale markets monitoring activity. These include:
- *Scale of activity:* The wholesale markets involve very high volumes of transactions being executed by large numbers of customers. The monitoring activity undertaken should therefore be adequate to handle the volumes undertaken by the firm.
 - *Use of multiple brokers:* Customers may choose to split execution and clearing services between different firms and many customers may use more than one execution broker on the same market. The customer's reasons for this include ensuring that they obtain best execution, competitive rates, or to gain access to a particular specialism within one firm. This will restrict a firm's ability to monitor a customer, as they may not be aware of all activity or even contingent activity associated with the transactions they are undertaking.
 - *Electronic execution:* There is an increasing use of electronic order routing where customers access markets directly and there is little or no personal contact between the firm and the customer in the day-to-day execution of the customer's business. This means that the rationale for particular transactions may not be known by the firm.
- 18.55 The nature and extent of any monitoring activity will therefore need to be determined by a firm based on an assessment of its particular business profile. This will be different for each firm and may include an assessment of the following matters:
- extent of execution vs clearing business undertaken;
 - nature of customer base (geographic location, regulated or unregulated);
 - number of customers and volume of transactions;
 - types of products traded and complexity of those products; and/or
 - payment processes (including payments to third parties, if permitted).
- 18.56 Firms should ensure that any relevant factors are taken into account in determining their monitoring activities, and that the programme is adequately documented and subject to periodic review on an ongoing basis. Given the bespoke nature of some wholesale market products and the difficulties in developing meaningful rules for electronic monitoring (e.g., a lack of typologies for the sector), it may well be appropriate for a firm to monitor manually. Firms should, however, be able to demonstrate the rationale for their monitoring strategy.
- 18.57 Firms relying on third parties under the ML Regulations to apply CDD measures **cannot** rely on the third party in respect of monitoring of transactions and the customer relationship.
- 18.58 Firms may wish to leverage existing surveillance frameworks established for the purposes of compliance with the Market Abuse Regulation (MAR)³², to assist in monitoring certain wholesale markets activities for unusual transactions which may constitute financial crime. Where suspicious trading activity is identified and the firm considers it necessary to file a suspicious transaction & order report (STOR), the firm should consider whether the filing of a suspicious activity report (SAR) under the Proceeds of Crime Act (POCA) is also appropriate.

³² <https://www.fca.org.uk/markets/market-abuse>

FINAL BOARD APPROVED

*F. Guidance on specific products**Securities**Product specific risks*

- 18.59 Securities are typically regarded as a lower risk asset class and are a typical product traded on the wholesale markets. Firms should, however, be alive to the risk of insider dealing and market abuse (and the subsequent laundering of the proceeds of such offences) in the context of securities trading.

Who is and is not the customer?

- 18.60 Customers wishing to transact securities on a DVP basis may do so through an executing broker that will generally settle with the customer's settlement agent/custodian. Under this arrangement, the customer elects to execute transactions through an executing broker and to clear the transaction through a separate settlement agent/custodian. The orders can either be placed directly by the customer or by an agent on behalf of the customer. Once the transaction is executed, the executing broker will settle with the settlement agent/custodian simultaneously once payment is received.
- 18.61 Both the executing broker and the settlement agent/custodian will have a relationship with the customer.
- 18.62 It is usually (but not always) the customer that elects to execute transactions through one or more brokers and to clear such transactions through a settlement agent/custodian and, to that end, selects both parties.
- 18.63 Where a firm acts as executing broker, the party placing the order is the customer for AML/CTF purposes. Where the party placing the order is acting as agent for underlying entities, they, too, may be customers for AML/CTF purposes. In this context, firms should have regard to paragraphs 18.23 to 18.27 of this chapter.
- 18.64 Where a firm acts as settlement agent/custodian, the customer on whose behalf the transaction is executed is the customer for AML/CTF purposes.
- 18.65 A common additional participant in a DVP arrangement is the customer's investment adviser or manager, to whom the customer has granted discretionary trading authority. Where a firm is acting as executing broker and there is an investment adviser or manager acting for an underlying entity, the CDD performed, and whether there is an obligation to identify the underlying entity, will depend upon the regulatory status and location of the adviser or manager. When considering whether it is necessary to undertake CDD on the underlying entity, firms should have regard to paragraphs 18.25 and 18.26 of this chapter.

Customer due diligence

- 18.66 Where the underlying entity is to be considered to be subject to CDD by the executing broker, a risk based approach to CDD can take into account the investment manager and/or the settlement agent/custodian's equivalent regulatory status, pursuant to Part I, paragraph 5.6.4. This may reduce the identity information or evidence requested and what the firm verifies. Firms should take the relationship with the Investment Manager and settlement agent/custodian into account in their own CDD on customers, rather than place full reliance on the settlement agent/custodian.
- 18.67 Given the information asymmetries likely to exist between an executing broker and settlement agent/custodian, when a firm is acting as settlement agent/custodian it would not be appropriate, from a risk-based perspective, to rely on an executing broker, even if this would be permitted under the ML Regulations. Settlement agents/custodians should undertake the CDD measures as set out in Part I, Chapter 5.
- 18.68 Where transactions are settled on a free of payment basis, firms should ensure that they understand the commercial rationale for this arrangement.

FINAL BOARD APPROVED*Monitoring*

18.69 See the general guidance on monitoring at section E above.

Money market instruments*Product specific risks*

18.70 "Money Market Instruments" is the term used to collectively cover foreign exchange (FX), interest rate products and term deposits. These instruments will typically be traded in the wholesale market between regulated financial institutions and large corporates (listed and private) and the money laundering risk may therefore be viewed as generally lower. However, this risk may be increased by matters such as:

- the nature of the customer (e.g. the customer's business);
- the customer's regulatory status (e.g. a sophisticated private investor);
- the purpose of the trading (e.g. hedging may be regarded as lower risk than speculative transactions);
- requests for payments to be made to third parties: for example, customers, particularly corporates, that need to make FX payments to suppliers and overseas affiliates.

18.71 When assessing the money laundering risk in such circumstances, a firm may want to take into account the nature of the customer's business and the frequency and type of third party payments that are likely to result from such business.

Who is and is not the customer?

18.72 See the general guidance in paragraphs 18.21 to 18.43.

Customer due diligence

18.73 FX (as well as many other traded products) is commonly traded on electronic trading systems. Such systems may be set up by brokers or independent providers. When a firm executes a transaction on these systems the counterparty's identity is not usually known until the transaction is executed. The counterparty could be any one of the members who have signed up to the system. Firms should examine the admission policy of the platform before signing up to the system, to ensure that the platform only admits regulated financial institutions as members, or that the rules of the electronic trading system mean that all members are subject to satisfactory anti-money laundering checks, and identify its counterparty and any associated risks (see paragraph 18.18).

Monitoring

18.74 See section E for general guidance on monitoring.

Financial derivatives*Product specific risks*

18.75 Financial products are utilised for a wide range of reasons, and market participants can be located anywhere within the world; firms will need to consider these issues when developing an appropriate and holistic risk-based approach. The nature, volume and frequency of trading, and whether these make sense in the context of the customer's and firm's corporate and financial status, will be key relevant factors that a firm will need to consider when developing an appropriate risk-based approach. Firms should also consider whether the particular derivative to be traded is consistent with its understanding of the customer's expected activity.

18.76 Where firms are trading commodity futures, they should be mindful of the fact that physical delivery may be required.

18.77 The risks between exchange-traded derivatives and OTC derivative products in the financial derivative markets are the same as those set out in paragraphs 18.10 to 18.15.

FINAL BOARD APPROVED

- 18.78 Some derivative products may be complex in nature and linked to a chain of underlying assets. On this basis, where the firm is facilitating the trade of a derivative product, it is not expected to have sight of the specific asset underlying the derivative.

Who is and is not the customer?

- 18.79 See the general guidance in paragraphs 18.21 to 18.43.

Customer due diligence

- 18.80 See the general guidance in section D.

Monitoring

- 18.81 See the general guidance in section E.

- 18.82 When assessing alerts triggered by a firm's surveillance or other monitoring procedures, firms may wish to consider the nature of the client, and whether the observed activity is consistent with the firm's understanding of that client's expected activity (see also paragraphs 18.44 to 18.45 on expected activity more generally).

Commodities

Product specific risks

- 18.83 Regulated firms that, in addition to physical commodity activity, undertake any business with a customer which amounts to a regulated activity (including business associated with physical commodities) will be subject to the ML Regulations, including being required to conduct CDD on the customer.
- 18.84 When implementing a risk-based approach and producing or reviewing risk assessments or the risk profile of a prospective customer, there are a number of areas which commodity market firms may want to take into account in addition to the more general matters set out in Part I, Chapters 4 and 5. These will include, but not be limited to:
- The wide range of different business interests which populate the commodity markets. The types of participants may typically include:
 - Producers (e.g. oil producers and mining firms);
 - Users (e.g. refiners and smelters);
 - Wholesalers (e.g. utility firms);
 - Commercial merchants, traders and agents; and
 - Financial firms (e.g. banks and funds).
 - These types of firm are illustrative and widely drawn and firms can be present in more than one category (for example, a refiner will be both a user of crude oil and a producer of oil products).
 - The instruments traded in the wholesale commodity markets can allow for the speculative trading, hedging and physical delivery of commodities.
 - There may be third party funding of transactions in the commodities markets. Also, where a bank is sending funds to a customer to purchase a physical commodity and the customer hedges the risks associated with the transaction in the derivatives market through a broker, the bank may guarantee the payment of margin to that broker; this results in a flow of money between the broker and the bank on the customer's behalf. However, both the party making the payment on behalf of the customer, and the party receiving the funds, will be regulated financial institutions.
 - Firms should also consider whether it is necessary to assess the potential higher risk of corruption, money laundering, fraud or sanctions issues associated with extractive industries or governmental licences in higher risk jurisdictions through its CDD processes.

FINAL BOARD APPROVED

- 18.85 The risks and potential mitigating factors should be taken in the round. The global nature of the commodity markets means that firms from potentially higher risk jurisdictions with a perceived higher money laundering risk are likely to have legitimate commercial interests. Understanding the role of a prospective customer in the market, and their reasons for trading, will help inform decisions on the risk profile they present (see paragraph 18.17).
- 18.86 When undertaking commodities business, firms should have particular regard to the sanctions guidance in Part III, to the guidance on financial sanctions produced by the Office of Financial Sanctions Implementation within HM Treasury³³, and to any relevant trade sanctions³⁴.
- 18.87 Based on the commodities being traded and jurisdictions involved, a firm may consider its obligations under its own policy statement pursuant to the Modern Slavery Act (2015)³⁵.

Who is and is not the customer?

- 18.88 See the general guidance at paragraphs 18.21 to 18.43.
- 18.89 Where business does not fall within the scope of the ML Regulations, e.g., shipping and chartering, it is entirely a matter for firms to decide what commercial due diligence they perform on their counterparties, and what due diligence they may wish to undertake to mitigate ML/TF and other financial crime risks (e.g. for the purposes of complying with applicable sanctions regimes).

Customer due diligence

- 18.90 See the general guidance at section D.

Monitoring

- 18.91 See the general guidance in section E. Firms should remain alert to the need to carry out sanctions screening (including screening the names of vessels etc.) as part of their ongoing monitoring in this area.

Structured products

Product specific risks

- 18.92 Structured products are financial instruments specifically constructed to suit the needs of a particular customer or a group of customers. They are generally more complex than securities and are traded predominantly OTC, although some structured notes are also listed on exchanges (usually the Luxembourg or Irish Stock Exchanges).
- 18.93 There is a wide range of users of structured products. Typically they will include:
- Corporates;
 - Private banks;
 - Government agencies; and
 - Financial institutions.
- 18.94 The money laundering risk associated with structured products is not generally considered to be high, because of the involvement of regulated parties and because trading in structured products is unlikely to be a particularly effective way to launder criminal proceeds. However, because of the sometimes complex nature of the products, they may generally be more difficult to value than cash securities. This complexity may make it easier for money launderers, for example, to disguise the true value of their investments. Firms should therefore remain mindful

³³ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/645280/financial_sanctions_guidance_august_2017.pdf

³⁴ See <https://www.gov.uk/government/organisations/export-control-organisation> and <https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions>

³⁵ <http://www.legislation.gov.uk/ukpga/2015/30/contents/enacted>

FINAL BOARD APPROVED

of their obligations when trading in structured products, and ensure that they carry out EDD where red flags are identified.

- 18.95 The complexity of the structure can also obscure the actual cash flows in the transaction, enabling customers to carry out circular transactions. Understanding the reason behind a customer's request for a particular product will help firms to assess the money laundering risk inherent in the structure.

Who is and is not the customer?

- 18.96 Transactions are normally undertaken on a principal basis between the provider (normally a financial institution) and the customer. Some structured products are also sold through banks and third party distributors (introducers). In the latter circumstances, it is important to clarify where the customer relationships and responsibilities lie (e.g. are the third parties introducing clients to the firm or distributing products on behalf of the firm) and to set out each party's responsibilities in relation to AML. Where a firm wishes to contract out its customer identification and verification obligation to a distributor, it should establish whose procedures are to be used (e.g. the firm's or the distributor's), satisfy the reliance requirements and establish monitoring procedures.

Customer due diligence

- 18.97 See general guidance on CDD in section D.

Monitoring

- 18.98 See general guidance on monitoring in section E.

19: Name-passing brokers in inter-professional markets

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

- 19.1 In the inter-professional markets, wholesale market brokers pass the names of customers from one principal to another, either by the traditional voice broking method or via an electronic platform owned by the broker. The broker passing the names takes no part in any transaction or trade between the two counterparties.
- 19.2 The activity enables the broker to use his wide range of contacts across the wholesale markets to provide liquidity to the market, by putting in touch principals with a wish to transact, but who may not have the broker's depth of information about willing counterparties. The use of a broker also allows pre-trade anonymity for those counterparties who do not wish their position to be made known to the wider market.
- 19.3 Wholesale market brokers can arrange transactions in any product permitted under the Regulated Activities Order, or which is covered by the Non Investment Products code, published by the Bank of England.

Different types of relationship

- 19.4 The names which may be passed by the broker are generally limited to entities subject to financial regulation, to corporates and to Local Authorities. Regulated entities may be subject to regulation by the FCA or by an overseas regulator; corporates may likewise be UK domiciled or based abroad; Local Authorities are generally UK-based.
- 19.5 In principle, transactions of all types may take place between any of these parties. There is no difference in how the name-passing takes place, although there is an awareness that standards of regulation and corporate governance will vary across jurisdictions.

What are the money laundering risks in name passing?

- 19.6 Across all wholesale markets, the vast majority of participants are known to the other market counterparties. Many participants are subject to financial regulation, and most corporates who are dealt with are listed, and subject to public accountability. In principle, therefore, the money laundering risk in name-passing is very low. The risk associated with name-passing relates to the resultant transactions and business relationships, which are covered by other parts of the sectoral guidance.

Who is the customer for AML purposes?

- 19.7 Wholesale market brokers are arrangers in the sense of a financial intermediary. The principals introduced by name-passing brokers, who subsequently enter into trades or transactions with one another, are each other's customer if the principal is subject to the ML Regulations.
- 19.8 The name-passing brokers themselves play no part in any transaction.

FINAL BOARD APPROVED*Customer due diligence*

- 19.9 Wholesale market brokers must identify, and verify the identity of, the principals they pass to other market participants.
- 19.10 Principals that are required to comply with the requirements of Part I, Chapter 5, due to their being subject to the ML Regulations, cannot look to name-passing brokers to undertake identity verification procedures on their behalf.
- 19.11 The principals must therefore take steps to obtain, appropriately verify, and record the identity of counterparties (and any underlying beneficiaries) “introduced” to them by name-passing brokers.
- 19.12 Where a counterparty “introduced” by a name-passing broker fails to satisfy a principal’s AML identity verification checks, the principal is responsible for informing the name-passing broker that the prospective counterparty cannot be accepted.

20: Brokerage services to funds

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

This sectoral guidance is intended for firms such as prime brokers, executing brokers and clearing brokers providing brokerage services funds, which may be regulated or regulated and based in jurisdictions which may or may not be assessed as low risk (“funds”). The guidance considers specific issues over and above the more general guidance set out in Part I, Chapters 4, 5, and 7, which such firms will need to take into account when considering applying a risk-based approach.

A firm’s business activities with such funds may also fall within the scope of other sectoral guidance, for example, sector 16: *Correspondent relationships*, sector 18: *Wholesale markets* and sector 9: *Discretionary and advisory investment management* (c.f. paragraphs 9.22 to 9.24). As such, this sectoral guidance should be read together with other applicable parts of the guidance.

Overview of the sector

- 20.1 A fund is a vehicle established to hold and manage investments and assets. A fund usually has a stated purpose and/or set of investment objectives. It is important to draw a distinction between funds that are personal investment vehicles (set up by private wealth management) and those for a commercial purpose with, usually unrelated, investors (e.g. hedge funds). However, as both types of fund can use the same structures, the line between the two may sometimes be hard to distinguish.
- 20.2 Funds will normally be separate legal entities, formed as limited companies, limited partnerships and trusts (or the equivalent in civil law jurisdictions), so that the assets and liabilities may be restricted to the fund itself. Sub-funds of an umbrella fund typically take the form of different classes of shares, fund allocations to separately incorporated trading vehicles or legally ring-fenced portfolios. Sub funds may or may not be separate legal entities from their umbrella fund. The investors in the funds are the beneficial owners and the source of funds.
- 20.3 Funds may also operate a “master/feeder” arrangement, whereby investors, from different tax jurisdictions, invest via separate feeder funds that hold shares only in the master fund. Feeder funds may also on occasion invest/deal directly and therefore a firm may provide services to a fund that is acting in its own right while at the same time being a feeder fund of another, master, fund.
- 20.4 Dependent upon the structure, a fund is controlled by its directors, partners or trustees. However, in most instances the powers of the directors, partners or trustees will be delegated to the investment manager. It is not unusual to find that the key personnel of a fund are also the key personnel of the investment manager.
- 20.5 The complexity of the structures and multiple relationships associated with funds can often give rise to particular difficulties/uncertainties. It is, therefore, important that a firm knows who it is dealing with (if that party is acting on behalf of the client) and is clear about what it needs to

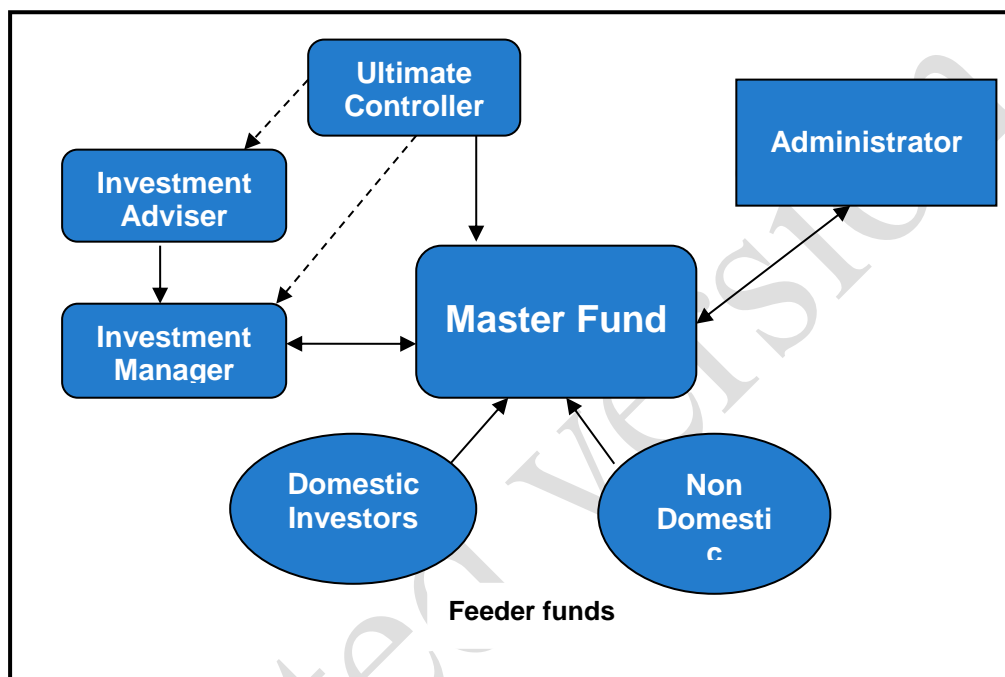
FINAL BOARD APPROVED

achieve: who are the client's principal controllers (e.g. who has the day-to-day decision making functions?) and the owners of the client's assets (who is investing into the fund(s)?).

Once these questions are answered, the precise steps to identify and verify the relevant parties will vary in each case.

- 20.6 The following diagram illustrates some of the key players in a fund, specifically a master feeder fund structure.

Note that the precise structure in each case will vary.



Note: both the Administrator and Investment Manager will usually act for the underlying feeder funds.

- **Ultimate Controllers**

The ultimate controller is someone who controls the funds/assets in the fund (e.g. the person who gives the orders). The ultimate controller may be a different person/entity in different fund set-ups but is usually not the beneficial owner. Sometimes it can be the investment manager, the adviser, or directors of other related parties, who may delegate this responsibility. Whilst the controller is not necessarily the owner, in personal investment vehicles it may be the voting shareholders, directors, holders of founding shares, who can sell or change the assets. The place to look for those who are the ultimate controllers is usually the fund's offering memorandum (although the documents provided at the account opening stage may not be final – see 20.18 below). Firms should also consider the legal agreements and ask who has control: ambiguity suggests more due diligence is needed.

- **Investment Manager**

Funds are managed by an investment manager, which is a separate legal entity to the fund, and which is given authority to act as agent and manage the funds and investments held by the fund vehicle. It is often the investment manager that will make investment decisions and place transactions with a firm as agent of the fund.

The investment manager plays a pivotal role within a fund structure, as it establishes and maintains the relationships with the Prime broker and the Clearing and Executing brokers and will, in most cases, be the direct contact with a firm on behalf of the fund. A firm may also act as investment manager to a fund in addition to providing other services (see section 9: *Discretionary and advisory investment management*).

Investment managers will usually be regulated but, depending upon the jurisdiction they are registered in or operate from, they may be subject to varying degrees of regulatory oversight. Firms should, therefore, satisfy themselves of the regulatory status and responsibilities of investment managers, in particular with respect to AML.

The relationship the investment manager has with investment advisers and ultimate controllers of the fund will vary depending upon the degree of control the investment manager has over the:

- a) selection of investors;
- b) investment strategy of the fund; and
- c) placement of orders.

A fund may have more than one investment manager, known as sub-managers. Sub-managers are responsible for managing/investing part of the fund, and, depending on the structure of the fund, there may be more than one sub-manager. Where investment management making decisions are delegated to sub-manager(s), CDD measures should be applied accordingly.

- **Investment Adviser**

Some funds appoint separate investment advisers who will advise the fund with regard to investment decisions undertaken on behalf of the fund, and on occasion, depending on the structure of the funds, may place orders with a firm. Where investment management making decisions are delegated to the investment adviser and/or where the firm is taking orders from the investment adviser, CDD measures should be applied accordingly.

- **Administrator**

Administrative services such as the day to day operation of the fund (e.g. valuations) and routine tasks associated with managing investments on behalf of investors (e.g. managing subscriptions and redemptions) will ordinarily be undertaken by a separate entity known as the fund administrator. Fund administrators may also perform the role of transfer agent and registrar. An administrator may be responsible for identifying and verifying the investors for AML purposes. In certain circumstances it might be appropriate to rely on the activities of the administrator in respect of the source of funds.

Fund administrators are often regulated/licensed (e.g., in Ireland) but their responsibilities may vary (e.g. depending on the domicile of the fund). Firms should, therefore, satisfy themselves of the regulatory status and responsibilities of administrators, in particular with respect to AML. The responsibilities of the Administrator are normally outlined in the Offering Memorandum/Prospectus.

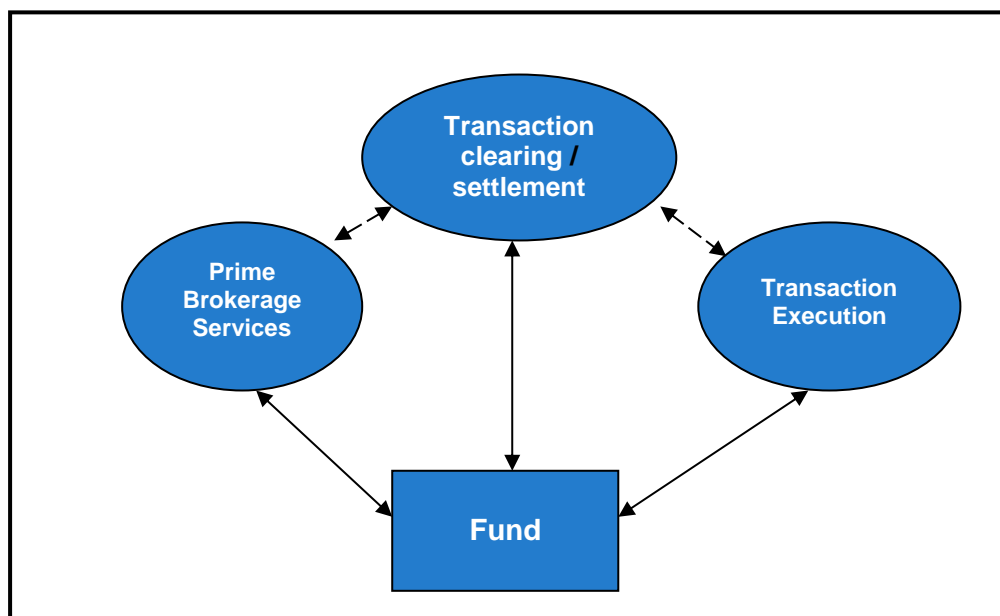
For some fund structures there may be different administrators for different feeder funds. It is important to identify all administrators whose responsibility it is to source investors and to apply due diligence measures accordingly.

- **Other Relationships**

FINAL BOARD APPROVED

In addition to the above-mentioned entities, who are involved with the operation and management of the fund, other parties may also be involved, such as auditors, law firms, trustees, and custodians. These parties may be less relevant to a firm meeting its AML obligations, but they may give a more complete picture of the fund set-up.

- 20.7 The following diagram sets out the likely services a firm may provide to a fund (although, as discussed above, the firm could deal with the fund via a number of entities).



- **Transaction Execution**

Transactions or trading are undertaken for a fund by a firm commonly known as an executing broker. A fund may elect to execute transactions through one or more firms. The executing broker takes instructions from the fund or its appointed agent (usually the investment manager), but passes the transactions/trades to a clearing broker for clearing and settlement.

- An executing broker may give up a transaction to a clearing broker for settlement (see section 18: *Wholesale Markets*).
- In transactions that involve delivery vs payment (DVP) cash or securities are swapped between the executing broker and settlement/clearing agent or, on occasion, the custodian.

An executing broker should be clear to whom they are speaking (i.e. who gives order) to and in what capacity, in order to determine whom they are facing.

The executing broker typically provides execution-only services to the investment manager and settles with a regulated prime broker(s).

- **Clearing/Settlement**

A fund may elect to execute transactions through one or more firms and elect to settle or clear such transactions through another firm known as the clearing broker. The clearing broker will settle the transaction/trades on behalf of the fund, and as

FINAL BOARD APPROVED

such will handle the movement of funds or assets from the fund in settlement of the fund's transactions and liabilities.

- **Prime Brokerage Services**

Prime brokerage is the provision of brokerage products and services to a fund. Prime brokerage is a portal to a suite of products and services offered by a prime broker such as custody, reporting, securities lending, cash lending and pricing (i.e. valuation services). Some prime brokers provide capital introduction, start-up services, credit intermediation, straight-through processing, futures and options clearing, research, contracts for difference and credit default swaps. Some funds may appoint more than one prime broker. The precise relationships will depend on the products and circumstances. However, it is important to recognise that although a prime broker takes equitable title to assets, where an executing broker is giving-up to a prime broker the credit risk to the executing broker is with the prime broker and the AML risk to the executing broker will be with the fund, investment manager etc.

- **Multiple function brokers**

A firm may undertake more than one of the prime, clearing and executing broker functions set out above, depending upon the structure set up for the fund by the investment manager.

What are the money laundering risks associated with funds?

20.8 Funds are perceived as attractive vehicles for money launderers. There are seven primary factors giving rise to this perception:

- The identity of those who invest into the funds will, in most cases, not be known to the firm providing services to the fund;
- An unregulated or possibly lightly regulated fund may make it more difficult to ensure that the AML requirements applied to investors are of the appropriate standard;
- A fund can have complex structures and consequently may appear to lack transparency of ownership and control;
- A fund offers a private agreement between investors and the fund, and has traditionally been subjected to limited, or no, regulatory oversight or control;
- Money flows in and out of a fund in the form of new subscriptions and redemptions of investors' interests (subject to the fund's subscription and redemption terms) and the bank accounts of the fund may be held offshore, sometimes in jurisdictions with banking secrecy;
- The volume and size of fund trading activity and the complexity of underlying trading strategies; and
- The fund may accept nominee investments.

How to assess the elements of risk

20.9 The level of risk actually posed by the fund will depend upon the nature of the fund and its transparency. The risks can be determined through undertaking appropriate customer due diligence, and in particular through understanding to whom the fund is marketed and its structure and objectives, as well as the track record and reputation/standing of the investment manager and/or other relevant parties in control of the fund.

FINAL BOARD APPROVED

- 20.10 The status and reputation of other service providers, such as executing, clearing or prime brokers, the administrator, auditors and law firms may be a factor in determining the risks associated with a fund.
- 20.11 Where a firm agrees to undertake third party payments on behalf of a fund, the risks of money laundering and fraud is increased. A firm should therefore ensure it has adequate procedures and systems-controls to manage the risk associated with those types of payments and receipts. A firm may wish to consider monitoring and/or undertaking periodic reviews of these types of payments and receipts, as well as ensuring appropriate levels of sign-off with the firm.

Understanding the Business for Risk Purposes

- 20.12 A firm should also consider, as part of its wider obligations in respect of financial crime and to mitigate reputational risk, whether there are any red flags that warrant further investigation. Some of the questions firms may wish to consider include, where relevant, whether the size and reputation of the service providers (administrator, investment manager, auditor, lawyers etc) match the funds profile and whether the due diligence procedures for investors into the fund appropriate?

Whilst structures associated with funds are often complex and involve a number of jurisdictions, an important question is: does it make sense? For example, why is a fund regulated and listed in different jurisdictions? Also, where, an administrator is located in a jurisdiction not assessed as low risk, or specific concerns have been identified, closer inspection of the administrator's due diligence activities and background should be considered.

Who is a firm's customer for AML purposes?

20.13

Who a firm should view as its customer, and who the firm should therefore subject to identification and verification procedures, may vary according to the business undertaken for funds. It is also important to recognise the answer to the question *who is the customer* may vary for FCA Conduct of Business and AML purposes. The following sets out examples of who may be viewed as the customer for AML purposes, and therefore should be subject to customer due diligence. Customer due diligence scenarios are also set out in Annex 20-I.

- Where the firm is acting as the investment manager or investment adviser³⁶ for a fund, see sector 9: *Discretionary and advisory investment management*.
- Where the firm is acting as an executing broker, the customer for AML purposes may be the fund, the investment manager, or both of them, depending upon the fund structure, the regulatory status of the parties and where appropriate the firm's risk-based approach and policies.

In particular, where the firm is acting for another party, for example, the investment manager, who is itself acting as agent for the underlying fund, the following should apply:

- Where the agent is appropriately regulated (or equivalent), they will be the customer for AML purposes, and there is no requirement to look to the underlying fund as a

³⁶ References to Investment Manager in this section also refer to Investment Adviser

FINAL BOARD APPROVED

customer, unless otherwise agreed by the parties. The investors into the fund are the beneficial owners.

- Where the agent is unregulated, or regulated within a jurisdiction not assessed as low risk, **both** the agent and the underlying fund will be considered to be the customer for AML purposes.
- The executing broker client definition and fund investor CDD requirements are set out below:

Parties involved	Investment Manager	Fund	Fund's investors
Investment Manager regulated in an assessed low risk jurisdiction (qualifies for simple due diligence)	Investment manager is a customer	Fund is a customer if there is a direct relationship with the firm	Identification of Fund's investors (or reliance) required, if fund is not determined to be subject to SDD
Unregulated Investment Manager or regulated in a jurisdiction not assessed as low risk	Investment manager is customer	Fund is a customer (even if there is no direct relationship)	Identification of Fund's investors required, if fund is not determined to be subject to SDD

- Where the firm is acting as clearing broker, settlement agent and/or prime broker the customer for AML purposes will be the fund. However, where a firm is taking instructions from the investment manager, the investment manager will also be a customer.
 - The clearing broker, settlement agent and/or prime broker client definition and fund investor CDD requirements are set out below:

Parties involved	Investment Manager	Fund	Fund's investors
Investment Manager regulated in an assessed low risk jurisdiction (qualifies for simple due diligence)	Investment manager is a customer (where a firm is taking instructions from the investment manager)	Fund is a customer	Identification of Fund's investors (or reliance) required, if fund is not determined to be subject to SDD
Unregulated Investment Manager or regulated in a jurisdiction not assessed as low risk	Investment manager is customer (even if firm has no direct relationship with Investment Manager)	Fund is a customer	Identification of Fund's investors required, if fund is not determined to be subject to SDD

FINAL BOARD APPROVED

- 20.14 Information collected by other departments in a firm, such as risk, operations, legal or credit may be helpful in ascertaining the risk. However, as discussed, above, different entities may be considered to be the counterparty for the purposes of, for example, credit risk, FCA Conduct of Business rules, AML.

Customer due diligence

- 20.15 Due to the characteristics of funds outlined above, in addition to applying CDD measures to the customer and (where simplified due diligence cannot be applied to the customer) the beneficial owners, it is appropriate to identify, depending on the risk, other parties involved such as the fund itself, its managers/advisers, and the fund's ultimate controllers and understand their relationships and roles.
- 20.16 On occasion, practical aspects of fund management are conducted onshore as a result of the delegation of responsibility for certain activities to onshore entities that may be subject to regulatory oversight. The interplay of these relationships needs to be assessed when determining the extent of due diligence necessary.
- 20.17 Depending on the services the firm is offering or providing to the fund, a firm should have particular regard to:
- Whether the firm is to have the Master Fund as its customer.
In such cases, firms will wish to obtain information from the Feeder Fund's offering memoranda/prospectuses and, in some instances, information on the fund's investors.
 - Whether a fund's ownership/control structure comprises numerous layers of entities and/or is transparent and understandable, and ensuring that the firm has a good understanding of the structure rather than focusing on the strict legal form alone. Who places orders and transactions on behalf of the fund or makes the investment decisions for the fund(s).
Often, this will be the investment manager, and the firm should review the investment management agreement to understand the scope of the manager's authority/control.
 - Whether there are any regulated or other reputable servicing entities in the fund set up.
- 20.18 The fund's prospectus, offering memorandum or other documents will set out details of the fund structure, appointed service providers - the investment manager, administrator, prime broker, lawyers and auditors - together with a summary of the material contracts such as the administration, investment management and prime brokerage agreements. If any documents are not final at the account opening stage, confirmation could be sought from an independent and reliable source attesting that key information will not change in the final version i.e. details of administrators, investment managers, or in the event they may change, the firm will be informed as soon as reasonably practicable. In this situation, a firm might decide, on a risk sensitive basis, to accept such confirmation. Final versions of the documentation should, however, be obtained and reviewed before the account is finally approved.
- 20.19 Where the fund has a number of layers of entities in its ownership/control structure (e.g. linked feeder and/or intermediate funds), to the extent practical and on the basis of a firm's risk-based approach, this chain and the inter-relationships between the parties, whilst not necessarily subject to the guidance set out in Part I, Chapter 5, should be established and documented.

FINAL BOARD APPROVED

- 20.20 Where the fund is the customer, the requirements for identification and verification of corporate structures, trusts, and individuals etc, which are set out in Part I, Chapter 5 should be applied to the fund.
- 20.21 A firm should also identify the entities involved with the fund on which it is required to carry out due diligence e.g. customers, beneficial owners. A firm may also wish to carry out commercial due diligence on other parties.

Investment manager

- 20.22 The identity of the investment manager that has direct contact with the firm, or which instructs the firm on behalf of the fund must be verified, in accordance with the guidance relevant to their entity type, set out in Part I, Chapter 5. Where simplified due diligence can be applied to the investment manager (see Part I, Chapter 5, section 5.4) there is no duty to identify the underlying customer (i.e., the fund or its relevant investors) provided the firm has no relationship with the fund (if it has, the firm will need to perform CDD on the fund and its relevant investors, but may wish to consider reliance (c.f. Part I, paragraphs 5.6.4ff). As discussed above, though, under its risk-based assessment a firm may consider it appropriate to identify other parties involved.
- 20.23 Where, however, an investment manager is unregulated or not regulated in an assessed low risk jurisdiction, the firm must undertake CDD on the investment manager (even if the firm has a customer relationship with the fund). A firm may also consider additional checks, which could include considering requesting or obtaining proof of exempt status where the investment manager is operating from a jurisdiction where similar entities are usually regulated.

Investors and relevant investors

- 20.24 Shares or units in funds may be open to general subscription, or to purchase by any qualifying investors. Alternatively, funds may be established for the exclusive use of a closed group of private investors. Whereas the Investment Manager usually ‘controls’ a fund, investors in a fund should be viewed as representing the ultimate source of funds of the customer. Firms should, therefore, consider whether or not there is a need for them to look at the underlying investors in such vehicles. This will depend up on the status of the fund (e.g. publically traded or private) and how it is operated in terms of dealing in its units/shares e.g. where such dealings are traded on a regulated market or exchange.
- 20.25 Where the fund is publicly traded, the underlying investors would be regarded as a class of beneficiary and so would not need to be verified individually. However, where the vehicle is being operated for private use by a specific group of individuals, those that have a 25% or more interest fund would be “relevant investors”, on whom CDD should be undertaken as beneficial owners (see Part I, Chapter 5, paragraph 5.3.8ff).
- 20.26 Although it will often be the administrators to the fund, it is important to establish who in the fund structure is responsible for the CDD process. If the party responsible for verifying the identity of the Relevant Investors is regulated in an assessed low risk jurisdiction and satisfies the definition of ‘third party’ in the ML Regulations, the firm may, in line with its own risk-based approach, be able to rely upon the third party to apply appropriate CDD measures (except monitoring) in respect of any Relevant Investors (see Part I, paragraph 5.6.4ff).
- 20.27 However, where the party responsible for the CDD process is not regulated in an assessed low risk jurisdiction, the firm should, as part of the determination as to the level of assurance necessary, also satisfy itself with regard the AML procedures of the responsible party.

20.28 Whether a firm has to identify and take risk-based and adequate measure to verify the identity of relevant investors, will, however, depend on a number of factors. In general terms, two scenarios can be distinguished depending on whether the firm has a business relationship with the investment manager and/or the fund:

(a) Customer relationship with the investment manager (*no relationship with the fund*)

(i) *Investment manager regulated in an assessed low risk jurisdiction*

- Where the investment manager is the firm's customer and simplified due diligence (SDD) can be applied to the investment manager (see Part I, Chapter 5, section 5.4) there is no duty to identify the underlying customer (i.e., the fund and its relevant investors (if any)) although, as discussed above, under its risk-based assessment a firm may consider it appropriate to identify other parties involved.

(ii) *Investment manager not subject to regulation in an assessed low risk jurisdiction*

- The investment manager cannot be relied upon under Regulation 39. Nonetheless, if the firm is able to satisfy itself on an ongoing basis that the CDD performed by the investment manager or by a regulated agent (e.g. administrator or transfer agent) is adequate and available to the firm on request, it may elect to re-use the due diligence work carried out by the investment manager. Otherwise the firm will need to undertake its own due diligence measures (including on any relevant investors).

(b) *Customer relationship with fund*

Where the fund is the firm's customer, then the firm may, if it considers it appropriate to do so under its risk-based approach, place reliance on a third party, which satisfies the definition in the ML Regulations, to perform CDD measures, including identification of beneficial owners (see Part I, Chapter 5, paragraph 5.6.18ff).

(i) *Investment manager, administrator or investment adviser regulated in an assessed low risk jurisdiction*

Subject to the firm's risk-based approach, a firm may take steps to establish that reasonable measures are in place within the fund structure for verifying the identity of Relevant Investors in the fund; obtaining assurances from that party that there are:

- Relevant Investors whose identity will be disclosed to enable the firm to take appropriate measures to verify their identity, or
- no Relevant Investors.

Where a firm accepts such a representation, this should be documented, retained, and subject to periodic review.

FINAL BOARD APPROVED

- (ii) *Investment manager (administrator or investment adviser etc) not subject to regulation in an assessed low risk jurisdiction*

The investment manager cannot be relied upon under Regulation 39 of the Money Laundering Regulations 2017 (“Regulation 39”). The firm will need to undertake its own due diligence measures (including on any relevant investors).

- 20.29 Where a firm is required to carry out its own due diligence on relevant investors - and/or following its assessment of the money laundering risk presented by the fund it feels it is not appropriate to place reliance on a third party - the firm must identify and verify the identity of Relevant Investors in accordance with the relevant guidance set out in Part I, Chapter 5, paragraph 5.3.8ff.

Start-up funds

- 20.30 On occasion, a firm may offer services to, or establish a relationship with, a fund that is a start-up. Start-up funds are funds that are in the pre-investor phase, and as such it is not appropriate to consider undertaking due diligence on the Relevant Investors; until the start-up phase is complete, the investors and their status as relevant or not, may change, depending on who else invests in the fund. In these circumstances, a firm should review the Relevant Investor situation and undertake, where appropriate, due diligence on Relevant Investors.

Feeder funds

- 20.31 At a minimum, the Feeder funds within a Master/Feeder structure should be identified in accordance with the guidance in Part I, Chapter 5. The entity responsible for AML/CTF due diligence at the Feeder Funds (ordinarily the Administrator, Registrar or Transfer Agent) should also be identified, as a firm may consider it necessary to place reliance on this entity pursuant with paragraph 20.26.
- 20.32 Feeder funds will own the assets/money held by the master fund. As the feeder funds will be investors in the fund, a firm should consider whether, under the ML Regulations or based upon its risk-based approach, the identity of the investors in the feeder funds needs to be verified, as Relevant Investors/beneficial owners.

Variations on Customer Due Diligence

Enhanced Due Diligence

- 20.33 In addition to the situations outlined in Part I, section 5.5, as part of a firm’s risk-based approach it may feel it necessary to undertake Enhanced Due Diligence on its customer and/or related parties e.g. a firm may consider obtaining independent validation from appropriate third parties.

Ultimate Controllers

- 20.34 Ultimate control may be exercised through a chain of entities between the fund and the ultimate controller. This relationship should be established and documented.
- 20.35 Where, because of the risk profile of the fund, a firm feels it appropriate to undertake Enhanced Due Diligence, the identity of the fund’s ultimate controller should be obtained and verified. Standard identity information in respect of the fund’s ultimate controller(s) where they are not the investment manager should be obtained, and the identity of the ultimate controller(s) should as appropriate be verified in accordance with the guidance for their entity type set out in Part I, section 5.3.

FINAL BOARD APPROVED

Feeder Funds

- 20.36 Where, because of the risk profile of the fund, a firm feels it appropriate to undertake Enhanced Due Diligence, the identity of the feeder fund should be verified in accordance with the guidance in Part I, Chapter 5, ensuring that the relevant investors of the feeder funds are subjected to the guidance set out in paragraphs 20.21ff.

Reliance on third parties

- 20.37 To avoid unnecessary duplication where an executing broker and a clearing broker are undertaking elements of the same exchange transaction on behalf of the same customer, which is not a regulated firm in an assessed low risk jurisdiction, the executing broker may be able to rely upon the clearing broker under the ML Regulations (see Part I, paragraphs 5.6.4ff) or otherwise take account of the fact that there is another regulated firm from an assessed low risk jurisdiction acting as clearing agent or providing other services in relation to the transaction.
- 20.38 Where a firm is acting as clearing broker or prime broker, from a risk-based perspective the firm should not rely upon a third party and should undertake full customer due diligence, including where relevant on beneficial owners, as set out in Part I, Chapter 5.

Monitoring

- 20.39 The money laundering risks to firms offering services to funds can be mitigated by the implementation of monitoring procedures. Guidance on the general monitoring requirements is set out in Part I, section 5.7. However, there are specific characteristics of funds which will be relevant, in particular the use of multiple brokers.
- 20.40 Customers may choose to allocate execution, clearing and prime brokerage between different firms and many customers may use more than one execution broker. The reasons for this include ensuring that they obtain best execution, competitive rates, or to gain access to a particular specialism within one firm. This will restrict a firm's ability to monitor a customer, as they may not be aware of all activity or even contingent activity associated with the transactions they are undertaking.
- 20.41 Monitoring funds' activity will be affected by the fact that firms may only have access to a part of the overall picture of their customer's trading activities. The fact that many customers spread their activities over a number of financial firms will mean that many firms will have a limited view of a customer's trading activities and it may be difficult to assess the commercial rationale of certain transactions.
- 20.42 The nature and extent of any monitoring activity will therefore need be determined by a firm based on a risk-based assessment of the firm's business profile. This will be different for each firm and may include an assessment of the following matters:
- Extent of business undertaken (executing, clearing, prime brokerage or a mixture of all three);
 - Nature of funds who are customers (e.g. geographic location);
 - Number of customers and volume of transactions;
 - Types of products traded and complexity of those products; and
 - Payment procedures.

FINAL BOARD APPROVED

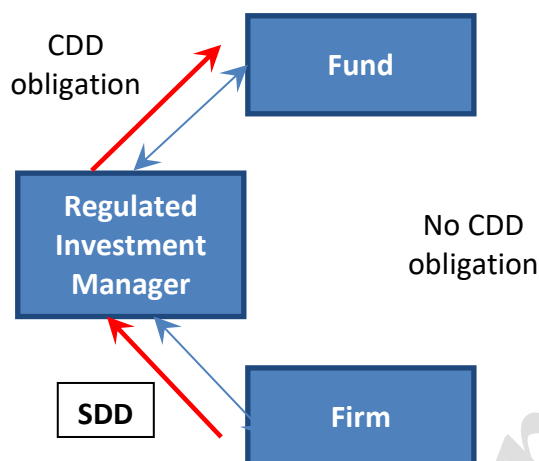
- 20.43 Firms should ensure that any relevant factors taken into account in determining their monitoring activities are adequately documented, and are subject to appropriate periodic review.
- 20.44 Firms relying on third parties under the ML Regulations to apply CDD measures cannot rely on the third party in respect of monitoring.

Outdated version

ANNEX 20-I

CUSTOMER DEFINITION DIAGRAMS

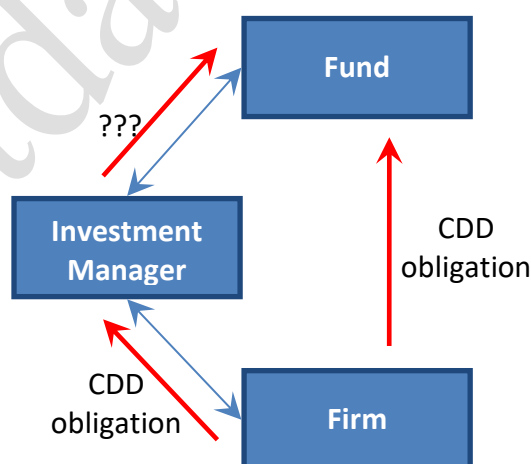
Diagram 1: Investment manager regulated in an assessed low risk jurisdiction



[Blue lines = customer relationship; red lines = CDD obligations]

The firm does not have a customer relationship with the Fund and receives instructions only from the investment manager. The firm is able to perform simplified due diligence (SDD) on the investment manager, subject to which it is not under any obligation to undertake CDD on the fund.

Diagram 2: Investment manager not subject to regulation in an assessed low risk jurisdiction

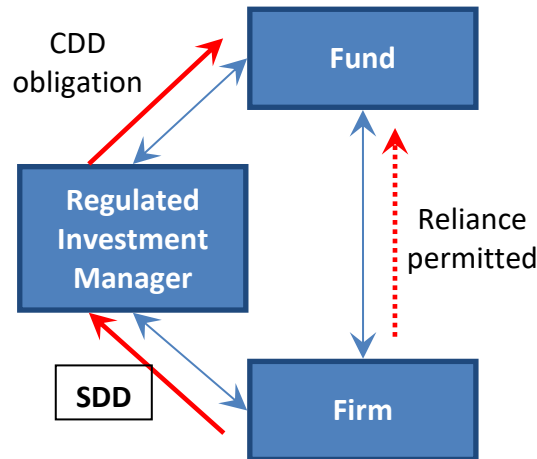


[Blue lines = customer relationship; red lines = CDD obligations]

The firm does not have a customer relationship with the fund and receives instructions only from the investment manager. It is, however, required to undertake CDD on both the investment manager and the fund on the behalf of

which the investment manager is acting (i.e. simplified due diligence is not available).

Diagram 3: Investment manager, administrator or investment advisor regulated in an assessed low risk jurisdiction

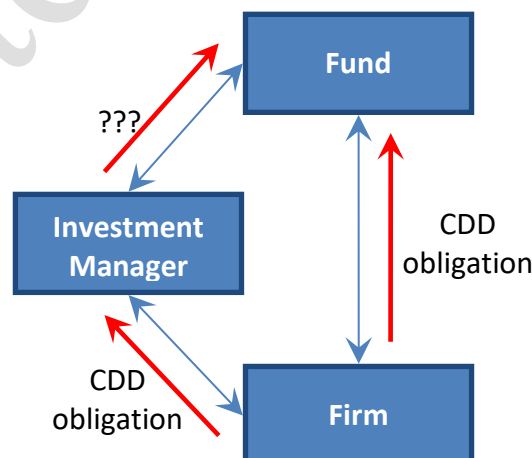


[Blue lines = customer relationship; red lines = CDD obligations]

The firm has a customer relationship with the fund, which has been introduced by the investment manager (investment adviser etc). The firm is required to undertake CDD on both the investment manager (investment adviser etc) and the fund.

However, the firm is able to apply simplified due diligence (SDD) on the investment manager and can, subject to consent by the investment manager, place reliance upon it for the purposes of CDD on the fund under Regulation 17. Similarly, a firm may be able to place reliance on a regulated administrator for CDD on the fund, provided the requirements of Regulation 17 are satisfied.

Diagram 4: Investment manager, administrator or investment advisor not subject to regulation in an assessed low risk jurisdiction



[Blue lines = customer relationship; red lines = CDD obligations]

The firm has a customer relationship with the fund, which has been introduced by the investment manager (or investment adviser etc). The firm is required to undertake CDD on both the investment manager (investment adviser etc) and the fund.

Outdated version

21 Invoice finance

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Products

- 21.1 Invoice finance companies offer a number of products to fund the working capital requirements of their clients; these generally fall into two categories – Factoring agreements and Invoice Discounting agreements. These can be operated on a Recourse or Non Recourse basis, and with or without disclosure of the assignment of the sales invoice to the client's customers, the debtors.

Factoring Agreements

- 21.2 *Factoring* is a contract between an invoice finance company and their client where revolving finance is provided against the value of the client's sales ledger that is sold to the invoice financier. The invoice finance company will manage the client's sales ledger and will normally provide the credit control and collection services. The client assigns all their invoices, as usually a whole turnover contract is used, after the goods or service has been delivered or performed. The invoice finance company will then typically advance up to 85% of the invoiced amount – the gross amount including VAT. The balance, less charges, is then paid to the client once the debtor makes full payment to the invoice finance company. The assignment is usually disclosed to the debtor, (although some contracts are operated on an agency basis, via the client, without disclosure of the assignment to the debtors and on occasions the management of the sales ledger can remain with the client as well).

Invoice Discounting Agreements

- 21.3 *Invoice Discounting* is a contract between the invoice finance company and their client where revolving finance is provided against the value of the client's sales ledger. The client will manage the sales ledger and will normally continue to provide the credit control and collection services. The client assigns all invoices, as usually a whole turnover contract is used, after the goods or service have been delivered or performed. The invoice finance company records and monitors this on a bulk sales ledger basis rather than retaining the individual invoice detail. The invoice finance company will then typically advance up to 85% of the invoiced amount. The balance, less any charges, is then paid to the client once the debtor makes full payment to the invoice finance company. The client undertakes the collection of the debt under an agency agreement within the contract. The client is obligated to ensure that the payments from debtors are passed to the invoice finance company. Where there is an agreement that the assignment is not disclosed, the colloquial title of Confidential Invoice Discounting is used to describe the undisclosed product, but confidentiality only exists at the discretion of the invoice finance company (whilst they are prepared to operate the agency arrangement).

Asset-Based Lending

- 21.4 Asset-Based Lending in the Invoice Finance industry would usually have the client's sales ledger at the core of the facility. It is a contract between the invoice finance company and their client where revolving finance and/or fixed amortising finance is provided against a 'basket' of assets – accounts receivables, inventory, plant machinery, property, etc.

FINAL BOARD APPROVED**Recourse Agreements**

- 21.5 *Recourse agreements* can apply to factoring or invoice discounting agreements. If the customer fails to pay the amount due to the client, then the invoice finance company will look to the client for reimbursement of any money they have advanced against that invoice.

Non Recourse Agreements

- 21.6 *Non-Recourse agreements* can apply to factoring or invoice discounting facilities. The invoice finance company effectively offers a bad debt protection service to the client. If the customer fails to pay the amount due to the client, due to insolvency, the invoice finance company stands the credit loss up to the protected amount, which is the value of the credit limit provided against the particular customer, less any agreed first loss amount.

Affiliated Factoring Companies

- 21.7 Assigned sales invoices may include overseas sales which require international credit control and collection services. Where the invoice finance company is not able to undertake this cross border activity, typically due to the lack of its own international network, it may enter into an arrangement with an Affiliated Factoring Company [AFC] in the appropriate country. This is often known as Export Factoring.
- 21.8 Affiliated Factoring Companies, operating in their own countries, will frequently have sales invoices with sales that require credit control and collection services to be performed in the United Kingdom. Where the AFC is not able to undertake this cross border activity, typically due to the lack of its own international network, it may enter into an arrangement with an invoice finance company in the United Kingdom. This is often known as Import Factoring.
- 21.9 The activities and associated risks are considered to be similar to correspondent banking* albeit are considered to be a lower risk, the financier being fully aware of the underlying transaction and the purpose of payment. For export facilities, the use of an approved AFC, in the country in which the debtor is domiciled also assists in reducing the risk associated with the transaction.
*See Part II, sector 16: *Correspondent banking* for specific guidance on the risks and controls applicable to this type of activity.

What are the money laundering risks in invoice finance?

- 21.10 As with any financial service activity, invoice finance products are susceptible to use by criminals to launder money. Both Factoring and Invoice Discounting products facilitate third party payments and may therefore be used by criminals for money laundering activity. The different invoice finance products available vary greatly and the degree of risk is directly related to the product offering.
- 21.11 The level of physical cash receipts directly received within the invoice finance sector is extremely low, as the vast majority of debtors settle outstanding invoices by way of cheque or electronic payment methods. Therefore the susceptibility of the invoice finance sector at the traditional placement stage is very low. The risk within the invoice finance industry is at the layering and integration stages of money laundering.
- 21.12 The main money laundering risks within the invoice finance sector are payments against invoices where there is no actual movement of goods or services provided, or the value of goods is overstated to facilitate the laundering of funds. As stated, the level of risk will depend upon the nature of the product and the level of involvement by the finance company. Factoring should be considered to be a lower risk than invoice discounting, in view of the fact that direct contact

FINAL BOARD APPROVED

is maintained with the debtor. Invoice discounting would represent an increased risk of money laundering due to the 'hands off' nature of the product.

21.13 The following factors will generally increase the risk of money laundering for invoice finance products:

- Cross border transactions
- Products with reduced paper trails
- Products where the invoice financier allows the client to collect the debt
- Confidential products
- Bulk products

21.14 The following factors will generally decrease the risk of money laundering for invoice finance products:

- Individual items (invoices, customers, receipts) being recorded and managed by the invoice financier
- Collections activity being undertaken by the invoice financier
- Non-recourse facilities
- Regular ongoing due diligence and monitoring including on-site inspections and verification of balances
- Regular statistical monitoring
- For export facilities, the use of an approved AFC, in the country in which the debtor is domiciled

21.15 Frequent occurrences, within the Invoice Finance sector, are short-term breaches of the underlying agreements by the clients. These are often due to client error or the clients' need for short term funding to cover a temporary deficiency. The vast majority of these short term breaches are not material in nature and the intelligence value of many of these occurrences, e.g., where invoices have been assigned prior to the actual delivery date by a matter of days, is extremely limited. However, the invoice financier should be aware that such instances could be one of the first indicators of the presence of money laundering and that a period of increased vigilance may be appropriate to ensure there is no reason to suspect money laundering.

21.16 The risks associated with short term breaches should be documented within the invoice finance company's risk assessment and appropriate controls established to ensure that, where there is a suspicion of the presence of money laundering, an appropriate report is filed with the NCA.

21.17 Invoice finance companies should recognise within their risk assessment that even though they may appear to be the only party affected by the client's, (or the client's customer's) action, the action in itself may represent an offence under POCA and as such the invoice finance company is obligated to file an appropriate report with the NCA.

Assessment of risk

21.18 It is important that each invoice finance company within its risk assessment has developed robust procedures to monitor the money laundering risks. Many of these procedures will overlap with those that are routinely used to manage credit risks within the sector, however other checks may need to be implemented, such as improved knowledge of the source of funds, that are different to the usual credit risk checks.

21.19 With extremely low levels of cash being transacted the susceptibility of the invoice finance sector at the traditional placement stage is very low.

FINAL BOARD APPROVED

- 21.20 Invoice finance products may be used to launder money at the layering and integration stages. However there are a number of factors that make the invoice finance facility less attractive to the money launderer, they are:
- The high levels of contact between the financier and the client, in terms of physical audits and visits, and of statistical monitoring
 - The sophisticated IT monitoring techniques used to detect issues with the quality of the underlying security, consisting of the quality of the goods and the customers (debtors),
 - In the case of factoring the item by item accounting and the regular direct contact with the debtors
 - The focus on the debtors in terms of creditworthiness and assessment of risk
 - The double scrutiny of payments, by the receiving bank and by the invoice financier
- 21.21 An invoice finance company operating a full factoring agreement, with regular contact, monitoring and review of the third party transactions, may determine that the risk level of Factoring Agreements, due to the level and frequency of the mitigating controls is low.
- 21.22 Invoice Discounting facilities, while generally considered higher risk than factoring facilities may also be characterised by regular due diligence by the Invoice Financier. The nature of these controls and the rationale for any reduction in risk assessment should be documented within the invoice finance company's overall risk assessment, which should be updated and reviewed on a regular basis.
- 21.23 Cross border transactions represent an increased risk of the presence of money laundering. The nature of the agreement will lead to these transactions being managed in different ways. This risk is reduced when the credit control procedures are managed by an approved AFC in the country in which the debtor is domiciled.
- 21.24 In general, the normally low to medium risk of money laundering will increase with the reduction of the levels of intervention by the financier and the increase in the size of foreign transactions through the account.

Who is the customer for AML purposes?

- 21.25 In the invoice finance sector the party with whom the factoring company holds a contract to provide finance is usually referred to as a 'client' and the client's customers as either 'debtors' or 'customers'. Therefore references in Part I of the Guidance to 'customer' refer to the client within the invoice finance sector.
- 21.26 The identification requirements on which guidance is given in Part I, Chapter 5 will only apply to an invoice finance company's clients – the parties with whom they have a contractual relationship. The client will be a business entity; a public limited company, private limited company, partnership or sole trader.
- 21.27 Whilst customers [the client's debtors] may be identified for routine credit risk or collection purposes by the invoice finance company, the requirement to identify, or verify the identity, of these customers does not apply.
- 21.28 Where invoice finance companies are involved in syndicated arrangements, the customer is as defined within Part II, sector 17: *Syndicated lending*. In such cases, the guidance in sector 17 should be read in addition to the guidance in this part of the Guidance.

FINAL BOARD APPROVED

- 21.29 Where invoice finance companies are involved in arrangements with Affiliated Factoring Companies (AFC) the AFC becomes the customer in an export relationship and the client in an import relationship. .

Customer Due Diligence

- 21.30 The CDD measures carried out at the commencement of the facility and the ongoing due diligence are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals using invoice finance facilities. Invoice finance companies should ensure that they coordinate both the identification and ongoing customer due diligence processes for clients in order to provide as strong a gatekeeper control as possible.
- 21.31 Invoice finance companies should carry out detailed initial CDD measures to gain a full understanding of the client and their business before opening a facility. This should be at a level to provide identification and establish expected activity patterns of their clients and their activities to meet the requirements set out in Part I, Chapter 5.
- 21.32 The identity of the client's debtors will normally only be obtained from the client, as part of the understanding of that client, without verification being required. The invoice finance company's risk assessment could determine that verification of the identity of some of the client's debtors will also be required under appropriate circumstances.
- 21.33 In terms of money laundering, some invoice finance products are considered higher risk than others; in these cases, enhanced due diligence measures are required.
- 21.34 Enhanced due diligence is appropriate in the following, but not exhaustive, list of situations:
- Where any party connected to the client is a PEP. See Part I, paragraphs 5.5.18-5.5.25.
 - When the client is involved in a business that is considered to present a higher risk of money laundering. Examples should be set out in the firm's risk-based approach and should reflect the firm's own experience and information produced by the authorities. See Part I, paragraphs 5.7.1-5.7.8 for guidance. These are likely to include the following, although this list should not be construed as exhaustive;
 - A client with any party associated with a country either on a residential or business activity basis that is deemed to have a relatively high risk of money laundering, or inadequate levels of supervision (see Part I, paragraphs 3.24-3.26). Examples of these countries can be found listed within the country assessments made by the International Monetary Fund or the Financial Action Task Force. Another source of information can be found within the Transparency International Corruption Perception Indexes that are published on an annual basis.
 - A client who carries a higher risk of money laundering by virtue of their business or occupation. Examples of which could be;
 - A business with a high level of cash sales.
 - A business with a high level of cross border sales, including Import-Export companies.
 - A business selling small high value goods that are easily disposed of.
 - Where transactions or activity do not meet expected or historic expectations, it is likely they will include the following:
 - Size – monetary, frequency, etc.
 - Pattern – cyclical, logical, frequency, amount, etc
 - Location – cross border, NCCT, rationale, etc.
 - Goods / Service – Type, Use, Payment norms, etc.

FINAL BOARD APPROVED

21.35 Monitoring aspects of enhanced due diligence should be set out in the invoice finance company's risk-based approach. It is likely they will include the following:

- More frequent and detailed on-site inspections of the client's books and records, frequently called an 'Audit', with appropriate management oversight and action of any significant deficiencies.
- More frequent and extensive verification, usually by telephone contact with the debtor, of the validity of the sale and invoice values.
- Greater management oversight of these facilities.
- Extended KYC