The Joint Money Laundering Steering Group

Prevention of money laundering/ combating terrorist financing

GUIDANCE FOR THE UK FINANCIAL SECTOR
PART II: SECTORAL GUIDANCE

December 2007

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

Specialist guidance

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 subsidiaries 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 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 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:

- Results of the FSA "Retail Cluster" work in 2002 – see www.fsa.gov.uk
- "International Students – opening a UK bank account" – see www.bba.org.uk
- FSA leaflet "Checking your Identity" – see www.fsa.gov.uk/pubs/public/identity_check.pdf

1.10 See also paragraphs 1.38 – 1.41 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 ensure that they 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.

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 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 The other documents cited in Part I, paragraph 5.3.74 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 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 1.22-1.24).

1.15 Standard due diligence is not required in the following situations:

- Where the source of funds may be used as evidence of identity. See Part I, paragraphs 5.3.92 to 5.3.96.
- Where a variation from the standard is required to prevent a person from being financially excluded (see paragraphs 1.38 – 1.41 and Annex 1-I).
- Products which meet the criteria in Regulation 9(8) and (9) of the ML Regulations 2007, e.g., a Child Trust Fund.

1.16 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.

1.17 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

1.18 If the existing customer was taken on pre-1994, or it could not be established that the holder's identity had previously been verified, an application would trigger standard identification procedures.

1.19 Most large firms have completed current customer review (CCR) checks. These could result in different levels of confidence in the identity of the person concerned, depending on the amount of information held on the existing holder. If the review had verified the customer's identity at least to the standard required as part of the CCR exercise, 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 passed current customer review checks, most firms would not require further identification.

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

1.20 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.

1.21 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.

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

1.22 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 5.3.74 and Annex 1-I).

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

1.23 Non-residents not physically present in the UK wishing to open an account in the UK are unlikely to wish to open a Basic Bank Account, with its limited facilities. The customer should be able to demonstrate a need for a bank account in the UK, or should 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 will apply where the customer is not met

personally or where other high risk factors come into play (see paragraphs 5.18-23 and Part I, section 5.5).

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

1.24 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

1.25 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 FSA authorised firms.

1.26 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

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

1.28 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, verifying the legal existence of the company.

1.29 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.

1.30 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.

1.31 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.

1.32 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.

1.33 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.

1.34 In determining the identification appropriate for partnerships (see Part I, paragraphs 5.3.212 - 5.3.225), 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.

Enhanced due diligence

1.35 Enhanced due diligence is required under Regulation 10 of the ML Regulations in the following situations:

- When the applicant is a PEP. See Part I, paragraphs 5.5.18 - 5.5.29.
- When there is no face-to-face contact with the applicant. An additional check is needed to offset the increased risk, notably that of impersonation fraud (see Part I, paragraph 5.3.82).
- When the business of the customer is considered to present a higher 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 3.24 – 3.26 and section 5.5 for general guidance.
- When establishing a correspondent banking 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).

1.36 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, or is conducted primarily on a non face-to-face basis. 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, hawala merchants
- 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)

1.37 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

1.38 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 5.3.110 to 5.3.114, and Annex 1-I.

1.39 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.

1.40 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.

1.41 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

1.42 Firms should note the guidance contained in Part I, section 5.7, and the examples of higher risk businesses in paragraph 1.36. 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.

1.43 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.

1.44 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.

1.45 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 FSA 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.

Training

1.46 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

1.47 Firms should note the guidance contained in Part I, Chapter 6. As indicated in Part I, paragraphs 7.31 to 7.33, further reference material and typologies are available from the external sources cited, viz: JMLSG, FATF and SOCA 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 SOCA.

1.48 There is no formal definition of what "as soon as practicable" means, but firms should note the enforcement action taken by the FSA in respect of the anti money laundering procedures in place at a large UK firm. The FSA 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 SOCA 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.

Interbank Agency Service

1.49 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 the Interbank Agency Service, 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 SOCA.

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.
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.
International students	Passport or EEA National Identity Card AND Letter of Acceptance or Letter of Introduction from Institution on the DfES list. 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 5.3.107-108.
Economic migrants *[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]*	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 www.homeoffice.gov.uk/. 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.
Refugees (those who are not on benefit)	Immigration Status Document, with Residence Permit, or IND travel document (i.e., *Blue* Convention Travel doc, or *Red* Stateless Persons doc, or *Brown* Certificate of Identity doc) 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.
Asylum seekers	IND Application Registration Card (ARC) *NB This document shows the status of the individual, and does not confirm their identity* 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. 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.
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 own Basic Account products, they should not lose sight of the requirement under *SYSC 3.2.6(G)(5)* "not unreasonably [to] deny access to its service to potential customers who cannot reasonably be expected to provide detailed evidence of identity."

ANNEX 1-II

(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……..

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. Payments can also be made to third parties that do not accept credit cards, by writing a cheque supplied on occasions by the card issuer. The amount of the cheque is added to the balance on the card account.

2.2 The cardholder agrees to repay any borrowing, in full or in part, at the end of each month. 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 month. 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, Switch/Maestro). 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.

<u>Different types of credit card</u>

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 very 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 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.

Merchant acquisition

2.9 Merchant Acquirers provide a payment card processing service, which facilitates customer debit and credit transactions between cardholders and merchants. Payment cards that bear card scheme acceptance brands (e.g., MasterCard, Visa and Switch/Maestro) are issued by banks and financial institutions which are members of the relevant card scheme. The Merchant Acquirer processes the transactions made by cardholders on behalf of its merchant customers, including, in appropriate cases, seeking authorisation requests from the card issuer when payments are made, and the facilitation of chargebacks, where a transaction is disputed.

2.10 Payment is made by the Card Issuer to the individual merchant's bank, which in turn settles with the merchant's account, normally via the clearing system. The individual merchant is therefore a customer of the bank with which it maintains a banking relationship.

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. For example, cash repayments, especially if by third parties, 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.

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

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
- 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.

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 5.3.119.

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 5.3.68 should be collected for all secondary cardholders and recorded in such a way that the data are readily searchable. Firms should aim to comply with this recommendation by the end of February 2008;

- 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 5.3.69, 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. The same will generally be true 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 FSA's guidance on outsourcing (www.fsahandbook.info/FSA/html/handbook/SYSC/8/9). 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.

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, or nationals of, 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

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.

The purpose of this sectoral guidance is to provide clarification to electronic money issuers on verification of identity and other customer due diligence measures requried by legislation. The guidance addresses products that are card-based as well as those that are entirely software-based.

This guidance may be used by all issuers of electronic money, regardless of whether they are regulated by the FSA or operate under a small electronic money issuers' waiver - (small issuers are subject to HM Revenue and Customs' regulation in relation to AML compliance).

What is electronic money?

3.1. The FSMA 2000 (Regulated Activities) (Amendment) Order 2002 amended the FSMA 2000 (Regulated Activities) Order 2001 to provide for the issuing of electronic money to be a regulated activity under FSMA. Electronic money is defined as:

> *'…monetary value, as represented by a claim on the issuer, which is:*
> *(a) stored on an electronic device;*
> *(b) issued on receipt of funds; and*
> *(c) accepted as a means of payment by persons other than the issuer.'*

3.2. 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 can be card-based or account-based and used entirely online.

3.3. Electronic money may be issued by banks or building societies with the requisite variation of permission from the FSA, or it may be issued by specialist Electronic Money Institutions, who obtain an authorisation from the FSA. The FSA also issues waivers to 'small e-money issuers' which meet the criteria set out in article 9 (C) of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544), as amended.

3.4. The Money Laundering Regulations 2007 apply to all issuers of electronic money in their capacity as financial institutions as defined in Regulation 3.

3.5. Electronic money may also be issued cross-border into the UK by EEA credit institutions holding the appropriate passport from their home state supervisor under article 28 of the Banking Consolidation Directive (2006/48/EC). In these circumstances, the issuer's AML procedures are regulated by the home state authorities.

Definitions

3.6. The following terms are used in this guidance:

- **Accounted/unaccounted products:**

  Accounted products are those that record centrally every transaction that takes place within the system. Such recording need not be in real time, and may be subject to cycles of clearing and settlement.

  Unaccounted products do not involve the central recording of every transaction, although transactions may be recorded at the point of sale, or point of transfer of value.

Accounted products may also comprise electronic vouchers that are not intended to be reloaded once used.

- **Card-based products:**

  These are products that employ a card or other electronic voucher for authentication, or to store the electronic money or a record of it on the card or voucher.

- **Closed/open scheme or system:**

  A closed scheme or system contains a single issuer of electronic money. There may, however, be multiple distributors or resellers, who purchase electronic money from the issuer for onward sale to consumers.

  An open scheme or system allows the participation of multiple issuers of electronic money, which means that there is a need for the clearing and settlement of transactions.

- **Complete information on the payer (CIP)**

  For the purposes of the Wire Transfer Regulation CIP consists of the payer's name, address and account number. The address may be substituted with the payer's date and place of birth, his customer identitifcaiton number or his national identity number. The account number may be substituted with a unique identifier. See Part II, Sectoral guidance A: *Wire Transfers*, paragraph A.14 for details.

- **Digital coin products:**

  These are unaccounted products where the product is distinguished by (a) a fixed denomination, (b) a unique digit string or serial number, and (c) the value residing in the electronic coin itself. The coin is usually discarded as soon as the electronic money is spent or redeemed.

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

  The EMA is the trade body representing electronic money issuers and 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.

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

  A PSP is defined in Article 2(5) of the Wire Transfer Regulation as "a natural or legal person whose business includes the provision of transfer of funds services".

- **Wire Transfer Regulation [also known as the Payer Regulation]:**

  Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds implements Special FATF Recommendation VII in EU member states. This guidance refers to it as the Wire Transfer Regulation, although this term has no formal standing. Supervision and enforcement provisions for this Regulation are implemented in the UK through the Transfer of Funds (Information on the Payer) Regulations 2007 (SI 2007/XXXX).

- **Purse:**

  An electronic money purse is a store of electronic money, which may be in an account, on a card or other device.

- **Redemption**:

This is the process whereby a customer submits electronic money to the issuer for exchange at par value, for cash, cheque or a fund transfer drawn on the issuer's account. (Note that the term is sometimes used in the gift card industry to indicate the spending of value with merchants).

- **Regulations, the:**

  The Money Laundering Regulations 2007 (SI 2007/2157)

- **Server-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, usually online.

  Note that Euro figures have been converted to approximate figures in Sterling, except where reference is made to legislative provisions.

Background to money laundering and terrorist financing risks related to electronic money

3.7. Electronic money is a retail payment product that is used predominantly for making small value payments. As an electronic means of payment, it is susceptible to the same risks of money laundering and terrorist financing as other retail payment products. In the absence of controls over the use of the product, there is a significant risk of money laundering taking place. The implementation of purse limits, useage controls, and systems to detect suspicious activity contributes to mitigating these risks.

3.8. Furthermore, where electronic money is limited to small value payments, the use of this product 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.

3.9. The electronic money products in commercial use today do not provide the kind of privacy or anonymity that cash provides, nor its utility. This is due to a number of factors: commercial practice, for example, dictates that most products are funded by payments from bank accounts or credit cards, and therefore can often reveal the identity of the customer at the outset. Similarly, use of these products often leaves an electronic trail that can help locate, if not identify, the user of a particular product.

3.10. As issuers of electronic money usually occupy the position of intermediary in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement investigations that complements identity data provided by other financial institutions. This may be equally or more valuable in the chain of evidence than a repetition of the verification of identity process, as it can yield valuable information to assist law enforcement in that event.

3.11. 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.

3.12. Risk factors that apply specifically to electronic money products are set out in paragraphs 3.15 and 3.16 - 3.18. Other risks set out in Part I of this Guidance also affect issuers (e.g., customer profile or geographical location of activity, see Part I, chapter 4 for details), and issuers are required to include these in the risk assessment that they undertake. Risk assessment should be an ongoing process and take into account information from transaction monitoring systems (see paragraphs 3.45 – 3.47). Issuers should manage the risks through carrying out appropriate customer due diligence measures.

3.13. The EMA publishes a typologies document, which outlines money laundering and terrorist financing risks and the means of mitigating them. This is a working document, which is updated on a regular basis. Issuers can obtain a copy of this document from the EMA by writing to information@e-ma.org.

3.14. This area of payments is evolving, and new products give rise to new risks. New mitigation strategies are therefore constantly needed. This will be reflected in the regular updates to this Guidance and other industry documents that are produced on a periodic basis.

Factors increasing risk

3.15. The following factors will generally tend to increase the risk of electronic money products being used for money laundering or terrorist financing:

- The higher the value and frequency of transactions, and the higher the purse limit, the greater the risk: the €15,000 threshold for occasional transactions provided in the Regulations may in this context provide a convenient comparator when assessing such risk;
- Frequent cross-border transactions, unless within a single scheme, can give rise to problems with information sharing. Dependence on counterparty systems increases the risk;
- Some merchant activity is particularly susceptible to money laundering, e.g., betting and gaming offer a number of opportunities either with or without the collusion of the merchant; and money service businesses are considered as susceptible to exploitation for money laundering and terrorist financing[1];
- Funding of purses using cash offers little or no audit trail and hence presents a higher risk of money laundering;
- The non face-to-face nature of many products also 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;
- Redemptions at ATMs, as well as any allowances for the payment of refunds in cash for purchases made using electronic money will also increase the risk;
- The ability of non-verified third parties to use the product increases the risk; and
- The technology adopted by the product may give rise to specific risks that should be assessed.

Factors decreasing risk

3.16. Electronic money products address the risks that are inherent in payments in a similar manner to other retail payment products - by requiring systems that detect unusual transactions and predetermined patterns of activity.

3.17. Additionally, the annual allowance for redemption of electronic money reduces the risk by allowing funds to enter the system, but only allowing a relatively small amount (€1,000) to exit without verification. This practice has the effect of making the electronic money product a less attractive means for money laundering.

3.18. An issuer will mitigate and therefore generally decrease the risk of money laundering through electronic money products, and increase the likelihood of its discovery if it has taken place, through putting in place systems and controls that may include those that:

- Can detect money laundering transaction patterns, including those described in the EMA typologies document;
- Will detect anomalies to normal transaction patterns;

[1] The Government's Financial Crime Strategy noted that one in five money laundering investigations, and one in three terrorist finance investigations, features the exploitation of Money Service Businesses.

- 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;
- 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;
- Deploy sufficient resources to address money laundering risks, including, where necessary, specialist expertise for the detection of suspicious activities; and
- 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 restrict redemption of electronic money into accounts held at such institutions.

Verification of identity

3.19. The Regulations state that for a business relationship and for occasional transactions (single or linked transactions of €15,000 or more, if not carried out as part of a business relationship) verification of identity must be carried out at the outset (see Part I section 5.2 on timing). This requirement includes verification of beneficial owners (the individuals who ultimately own or control the customer or on whose behalf a transaction or activity is being conducted – see Part I, paragragraphs 5.3.8 to 5.3.13).

Merchants

3.20. 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:

- 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.

3.21. Issuers may allow merchants to benefit from the £1,650 turnover and £650 redemption allowance in order to enable the online recruitment of small merchants. This does not, however, alter the requirement to undertake adequate due diligence of the merchant's business.

Multiple-card products

3.22. 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.

3.23. Issuers with such products must mitigate the greater risk of money laundering to which these products are exposed by implementing systems and controls that seek to identify transactions or patterns that fit money laundering typologies for such products, and to act promptly to prevent money laundering.

3.24. Verification of identity for a second cardholder contributes to mitigating the risk, and should be considered even where there is no business relationship with that person.

One-off transactions

3.25. The purchase of a non-reloadable card or cards is a one-off transaction when it is not clear to the issuer whether the customer will return and make a repeat purchase of another card or cards. Such transactions for non-reloadable cards can then be regarded as one-off, for the purposes of this guidance.

3.26. A reasonable maximum purse limit should, however, be adopted for such products, and this should not exceed £650. Such cards should not, however, allow for redemption of electronic money without verification of identity taking place, subject to a £100 de minimis allowance.

3.27. These limits do not apply where there is a suspicion of money laundering or terrorist financing. In such circumstances, the identity of the customer must be verified, irrespective of the transacted total.

Customer Due Diligence

3.28. Guidance on verifying the identity of individuals and companies or other businesses in both face-to-face and non face-to-face circumstances, using documentary or electronic evidence, is set out in Part I, chapter 5. Detailed guidance for verifying the identity of customers who do not have access to a bank acount, or who lack credit or financial history, is provided under the financial exclusion provisions of Part I, section 5.3.

3.29. Issuers will also need to satisfy themselves that they meet the requirements of sanctions legislation. Guidance on this is provided in Part I, paragraphs 5.3.41 – 5.3.64.

3.30. Taking account of the risk mitigation features applied to electronic money systems, the approach to verifying identity for the electronic money sector is predicated on the need to minimise barriers to take-up of these new products, whilst addressing the risk of money laundering and meeting the obligations set out in the Regulations.

3.31. The Regulations require that electronic money issuers, in common with all financial sector firms, must carry out CDD measures on a risk-based approach.

3.32. Issuers are, in common with other financial services providers, required to verify identity at the outset of the relationship with the customer.

3.33. The Regulations specify circumstances where *simplified due diligence* can be applied. Simplified due diligence is an exemption for certain low-risk products from the requirement to apply customer due diligence measures. A purse must meet specific maximum storage, turnover and redemption limits in order for simplified due diligence to apply (see paragraphs 3.36 to 3.42). Where a product qualifies for simplified due diligence, there are no requirements for having to verify the customer's identity. As part of a basic risk-based approach, however, firms must have systems in place to detect abuse of the turnover alowance and other suspicious transaction patterns etc. (see paragraph 3.45), Once the limits are reached, issuers are required to undertake verification of identity on a risk-sensitive basis (see paragraph 3.43).

3.34. *Enhanced due diligence* is required to be carried out in higher risk situations. One of these situations is where the customer is not physically present to be identified by the issuer. Whether and what enhanced due diligence measures are required of the issuer will depend on the facts – (see paragraphs 3.57 – 3.60).

3.35. If a product qualifies for simplified due diligence, no verification of identity is required, even where the customer is not present, so long as no exceptional factors apply.

Simplified due diligence

3.36. The Regulations describe the simplified due diligence provisions for electronic money at Regulation 13 (7)(d):

> *'(d) electronic money, within the meaning of Article 1(3)(b) of the electronic money directive, where:—*
> *(i) if the device cannot be recharged, the maximum amount stored in the device is no more than 150 euro; or*
> *(ii) if the device can be recharged, a limit of 2,500 euro is imposed on the total amount transacted in a calendar year, except when an amount of 1,000 euro or more is redeemed in that same calendar year by the bearer (within the meaning of Article 3 of the electronic money directive).'*

3.37. **Non-reloadable purses:** where electronic money purses cannot be recharged, and the total purse limit does not exceed €150, verification of identity does not need to be undertaken. This takes into account the ability of individuals to purchase multiple purses and to therefore accumulate a higher overall total of purchased value.

3.38. This behaviour will, for example, be expected for gift card products. The purchase of electronic money gift cards is likely to be undertaken in multiple numbers, because of the nature of the product. Provided that the gift card does not allow for redemption to be made at ATMs, 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, on a risk weighted basis, without identity being verified.

3.39. **Reloadable purses:** those issuers that provide electronic money purses that can be recharged, whether card or purely server-based, are therefore required to undertake verification of identity procedures only when the annual turnover limit of £1,650 is exceeded, or if the customer seeks to redeem more than the £650 annual allowance.

3.40. Where purses can both send and receive payments, such as, for example, in online account-based products that enable person to person payments, the £1,650 turnover limit is applied separately to sending and receiving transactions. In other words, the turnover limit is calculated separately for credit and debit transactions, and the verification requirement applied when either of the two is exceeded.

3.41. Additionally, and in order to address obligations arising from the Wire Transfer Regulation, issuers must verify the identity of customers seeking to undertake any single sending transaction that exceeds £650 in value, where verification has not already been undertaken (see paragraph 3.64).

3.42. In summary, under simplified due diligence, identity verification must be undertaken on a customer with a reloadable purse on his:

- Reaching the cumulative annual turnover limit of £1,650; or
- Reaching the annual redemption limit of £650; or
- Seeking to undertake a single sending (debit) electronic money transaction which exceeds £650; or
- Where the issuer suspects money laundering or terrorist financing.

3.43. In respect of products benefitting from simplified due diligence, identity must be verified before cumulative turnover limits are exceeded. Systems must therefore be in place so that issuers are able to anticipate the approach of limits and to seek identification evidence in good time, before the annual turnover limits are reached. Firms must freeze the account if the limits are reached before verification of identity has been completed.

Basic requirements under this Guidance for a risk-based approach

3.44. This Guidance provides for additional measures that issuers are required to meet as part of the basic application of a risk-based approach. These measures are:

Verification of identity

(i) Either the electronic money scheme is a closed system; or

(ii) It is an open system, in which case all other participating issuers should under this Guidance also meet these requirements;

a) In all cases merchants must be subject to due diligence measures in accordance with Part I, Chapter 5 (but see paragraph 3.21 for a limited exemption).

b) Where electronic money is accepted by merchants or other recipients belonging to a wider payment scheme (for example Visa or MasterCard), the issuer must satisfy itself 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 regulation.

c) Where redemption of electronic money is permitted by way of cash withdrawal at ATMs or through a cash-back facility at retailers, and where this can exceed the annual redemption limit of £650 or single transaction limit of £650, verification of identity must be conducted at the point of issuance of the electronic money. Furthermore, issuers must 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.

d) Purse controls (e.g., turnover velocity, purse limits) must be implemented in such a way that the utility of products for money laundering is decreased.

Monitoring

3.45. The principle of monitoring of a business relationship is an obligation under the Regulations. As part of a risk-based approach, issuers must 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;
- Systems that identify discrepancies between submitted and detected information – for example, between country of origin submitted 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 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 rules that specify 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; and
- 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 produced by the EMA.

3.46. Issuers will need to evidence that they deploy an adequate range of controls for the type of risks that they encounter. Information obtained through monitoring should be reviewed as part of the ongoing risk assessment associated with the use of these products, and issuers should take action to enhance customer due diligence, for example that of verification of identity, where there are higher risks.

3.47. Issuers are reminded that in the event that potentially suspicious activity is detected by internal systems or procedures, the issuer must have particular regard to its obligations under POCA and the Terrorism Act (see Part I, Chapter 6) to report possible money laundering or terrorist financing.

Basic requirements under this Guidance for customer due diligence

3.48. As stated in paragraph 3.31, the Regulations require that CDD measures are carried out on a risk-based approach, as set out in Part I, Chapter 5. Electronic money is issued in a range of products, for a range of purposes covering a spectrum of risk – from the purchase of goods and services, to person-to-person payments. An issuer's risk-based approach to CDD measures will, as required by the Regulations, depend on the type of product or transaction involved.

3.49. As part of a risk-based approach to verification of identity, the Regulations require that verification is carried out on the basis of 'documents, data or information obtained from a reliable and independent source'. A customer's funding instrument (such as a credit card or bank account) can constitute such data or information.

3.50. A funding instrument on its own, however, is a weak form of verification of identity, first, because the credit or financial institution whose evidence is being used upon may not have verified the customer to current standards, and secondly because there is a risk that the person using the account may not be its rightful holder. This second risk is even higher where an electronic money issuer has no evidence that the account is held in the same name as the customer, such as for example in relation to direct debits.

3.51. Use of the funding instrument as evidence should therefore only be made where the circumstances are judged to be low risk (see paragraphs 3.15 - 3.18 for guidance on factors that increase or decrease risk), and verification of identity for any product may only be satisfied if:

a) The firm has in place the systems and processes set out in paragraph 3.52.

b) The funds to purchase electronic money are drawn from an account or credit card with, or issued by, a credit or financial institution[2] in the UK, the EU or an equivalent jurisdiction, which is supervised for its AML controls;

c) 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 paragraph 3.54); and

d) The purse does not exceed a maximum turnover limit of £10,000 from the commencement of the business relationship; and

3.52. The systems and processes which must be in place include:

- Those necessary for identifying incidents of fraudulent use of credit/debit cards and bank accounts.
- Those that enable monitoring to identify increased risk for such products, even within the permitted turnover limits. If the risk profile can then no longer be regarded as low risk, additional verification requirements must be taken.
- Recording of additional information such as IP addresses should be undertaken to assist in determining the electronic footprint of the user.

3.53. Collectively, the processes set out in paragraph 3.51(a) to (c) are intended to compensate for the weakness of using a funding instrument as evidence of identity without additional means of ensuring its integrity and its authorised use.

3.54. Where payment from a funding institution 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:

- 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, 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 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.

[2] Other than an MSB or a firm holding only a CCA licence

- Issuers may also use additional anti-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.

- 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 period of time is 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 six 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[3].

3.55. Furthermore, electronic money issuers should have processes in place to ensure that additional due diligence steps are undertaken if the risk posed by the product or customer increases so as to pose a higher risk of money laundering or terrorist financing (see paragraph 3.15). In such circumstances, where the risk posed can no longer be regarded as low, issuers must augment the basic approach to verification with other means of verification, such as those provided in Part I, Chapter 5.

3.56. To this extent, and in other circumstances, complete information on the payer, received as part of the obligations under the Wire Transfer Regulation, may also contribute to verifying a customer's identity

Enhanced due diligence

3.57. The Regulations 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, as well as in respect of business relationships or occasional transactions with politically exposed persons (PEPs).

3.58. Where electronic money purses[4] 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 (Part I, paragraphs 5.5.10 to 5.5.17 provide guidance on enhanced due diligence for non face to face transactions.).

3.59. What measures are taken will depend on a number of factors, including an asessment of the risk posed by the product itself. Issuers may adopt means of verification other than those outlined in Part I, including those outlined at paragraphs 3.51 to 3.56.

3.60. The degree of enhanced due diligence required for PEPs will be proportionate to the risk posed by the product, as will the requirement for systems and processes to detect PEPs. Where electronic money transactions and cumulative turnover values are low, the risk posed by way of their use by PEPs for money laundering is also likely to be low. Issuers should therefore 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 at Part I, paragraphs 5.5.26-5.5.29.

[3] The six month period should be completed before the limits associated with SDD (see paragraph 3.36) are exceeded.

[4] If an electronic money purse meets the conditions for simplified due diligence, no identification of the customer is required, even though the customer may not have been physically present.

Transition

3.61. Issuers must apply customer due diligence measures at appropriate times to their existing customers (as at 15th December 2007) on a risk-sensitive basis, unless the product qualifies for simplified due diligence. Card-based products that are already in issue under the old Guidance provisions may continue to operate until their existing expiry date is reached. When they are replaced, however, the new cards must be subject to the new cumulative turnover, transaction and redemption provisions provided under this Guidance.

Wire Transfer Regulation

3.62. General provisions for compliance with the Wire Transfer Regulation are provided in Part I, paragraphs 5.2.10ff *Electronic Transfer of funds*, and Part II, Specialist guidance A: *Wire transfers*.

3.63. Issuers are subject to the obligations of the Wire Transfer Regulation in their role as PSP of the payer, PSP of the payee and intermediary PSP. An overview of these requirements is provided schematically at Appendix I to this Guidance.

3.64. Payments using electronic money and funding of purses:

(i) Transactions below £650 in value do not require the collection or sending of Complete Information on the Payer (CIP), as these transactions are subject to the exemption provided by Article 3(3) of the Wire Transfer Regulation.

(ii) Transactions exceeding £650 in value require the collection and verification of CIP on a risk-weighted basis as set out elsewhere in this Guidance or as set out at A11-A14 of Part II, Specialist guidance A: *Wire transfers*.

(iii) Where an electronic money purse is funded through a card payment exceeding £650, it has been agreed that for practical purposes such a transaction consitutes payment for goods and services under Article 3(2) of the Regulation, and consequently the sending of the card PAN number satisfies the requirement for a unique identifier to accompany the transfer of funds.See Part II, Specialist guidance: *Wire Transfers*, paragraph A19. However, subsequent payments from the electronic money purse must be in accordance with (i) and (ii) above.

(iv) When funding transactions exceeding £650 are made from a bank account or other financial institution account in the EU, then CIP can be substituted for, with an account number or a unique identifier enabling the transaction to be traced back to the payer (see Article 6 of the Wire Transfer Regulation).

3.65. Redemption of electronic money:

(i) 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. Issuers may, however, attach customer (in addition to their own) CIP 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.

(ii) Where redemption is made in cash, this benefits from the exemption from the Wire Transfer Regulation for cash withdrawals from a customer's own account provided byArticle 3(7)(a).

3.66. Verification of identity for CIP information should be undertaken on a risk-weighted basis as provided for elsewhere in this Guidance or as set out in paragraphs A11-A14 of Part II, Specialist guidance A: *Wire transfers*.

Industry practice

3.67. A summary of good industry practice is provided in the table below.

3.68. It should be noted that the annual cumulative turnover limit of a purse is interpreted as the greater of either the total amount of electronic money sent by a purse or the total amount of

electronic money received by a purse, and includes any purchase value that is credited to the purse. 'Annual' refers to 12 month periods from the opening of the purse.

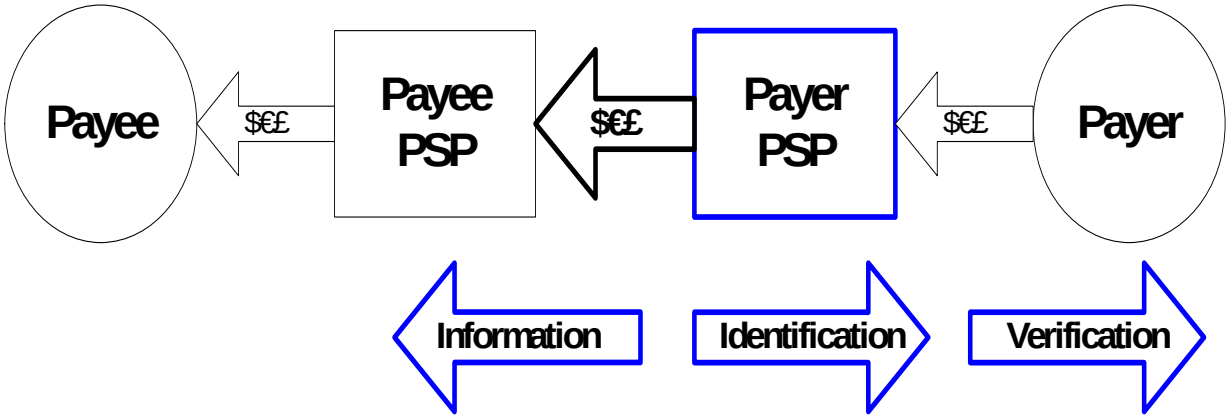
3.69. Finally, issuers are reminded that the responsibility for AML compliance always rests with the regulated issuer itself. When an issuer uses agents or outsourced third parties to undertake any of the CDD measures on its behalf, the issuer continues to be responsible for meeting the requirements of the Regulations.

Product Characteristics	Industry Practice	Comments
Electronic money products that have not implemented the purse limits and requirements set out in paragraphs 3.36 and 3.44, and allow transactions in excess of £650 to take place. The products enable either or both consumer-to-merchant and consumer-to-consumer payments.	Issuers should undertake: - Due diligence of customers at the outset; and - Due diligence of merchants at the outset. Issuers must also have systems in place to monitor and detect incidents of potential abuse, such as the opening of multiple accounts by a single individual or the opening of consumer accounts by merchants.	Appropriate measures will vary according to product and circumstances. Possible measures include further customer due diligence measures where there is a high risk of money laundering or terrorist financing, restrictions on functionality or turnover of purses, or more frequent monitoring.
Issuers should consider the practices below in the context of the risk factors set out in paragraphs 3.15 - 3.18, and adapt these practices as appropriate to take account of greater risks.		
Electronic money products that have implemented the purse limits and requirements set out in paragraphs 3.36 and 3.44, and limit the size of transactions to a maximum of £650. The products enable either or both consumer-to-merchant and consumer-to-consumer payments.	Where annual turnover is limited to £1,650, redemption to £650 and individual transactions to a maximum of £650, consumers do not need to be verified. Identity of customers to be verified on requesting redemption of a value exceeding £650. Verification of identity required as the annual £1,650 limit is approached – purse frozen if identification evidence not provided. Verification of identity required if the £650 transaction limit is exceeded. Merchants may also benefit from the annual £1,650cumulative turnover and £650 annual redemption limits, subject also to the £650 transaction limit. Notwithstanding this, Merchants' identity should wherever possible be verified at the outset and in all cases	Benefits of product include: - Cost of verifying identity not borne where product is used only once or occasionally; - No delay and little or no barrier to sign up of new customers; and - Privacy limited to consumers. Where customers act as merchants (e.g., in on-line auctions) but are not registered as merchants, and there is no reason to believe they are merchants, they may be considered consumers but are subject to the cumulative turnover limit.

Product Characteristics	Industry Practice	Comments
	appropriate customer due diligence measures carried out. Issuers must also have systems in place to monitor and detect incidents of abuse, such as the opening of multiple accounts by a single individual or the opening of consumer accounts by merchants. A full list of requirements is provided at paragraphs 3.44 – 3.45.	
Electronic money products that are non re-loadable and have implemented the purse limits set out in paragraphs 3.37 or 3.26, and limit the size of transactions to a maximum of £650. The products enable either or both consumer-to-merchant and consumer-to-consumer payments.	Merchant provisions are the same as those for re-loadable products above. Issuers must have systems in place to monitor and detect incidents of abuse, such as the opening of multiple accounts by a single individual or the purchase of multiple cards, or opening of consumer accounts by merchants. A full list of requirements is provided at paragraphs 3.44 – 3.45.	As above, for re-loadable products. Where customers have been subject to full due diligence, the purse limits for non re-loadable products can be increased, subject to the usual risk management considerations.

Appendix I

Scenario 1: Transfer of funds – Obligations on Payer PSP



Information

If to PSP outside the EU:
- Complete information

If batch file from single payer to PSP outside the EU:
- Complete information on batch
- Account number (or unique identifier) on single transaction

If both PSPs within the EU:
- Account number (or unique identifier)

Identification

Complete Information (CIP):
- Name
- Address (or date and place of birth, or customer identificatio number or national identity number)
- Account number (or unique identifier)

Verification

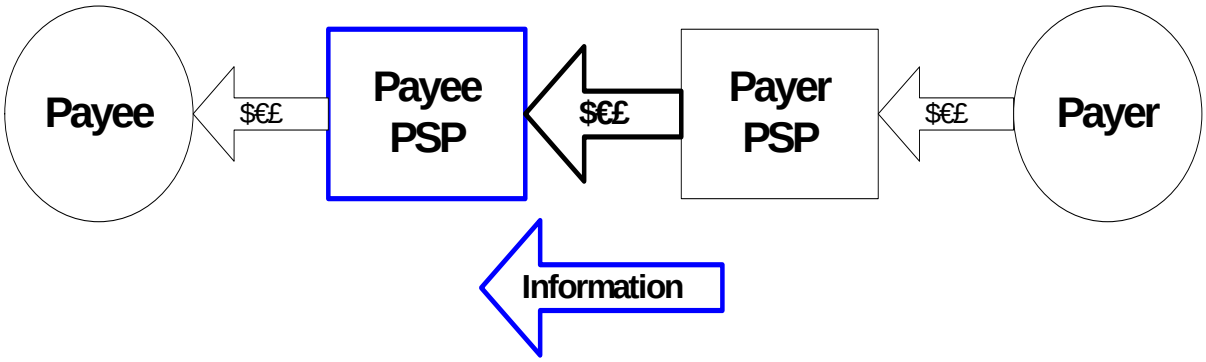
If transaction not from account with PSP:
- If below £650: No mandatory verification of CIP.
- If exceeds £650 or series of linked transactions exceeding £650: Verify CIP.

If transaction from account with the PSP (for any value):
- Verification deemed to have taken place if identity of account holder verified to meet AML requirements.

Records of CIP which accompanies transfer of funds to be kept for 5 years.

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.

Scenario 2: Transfer of funds – Obligations on Payee PSP



Procedures:
- Detect whether appropriate type of information attached and whether fields complete

If fields incomplete or information inappropriate:
- Ask for information or reject transaction
- Decide whether to report to law enforcement

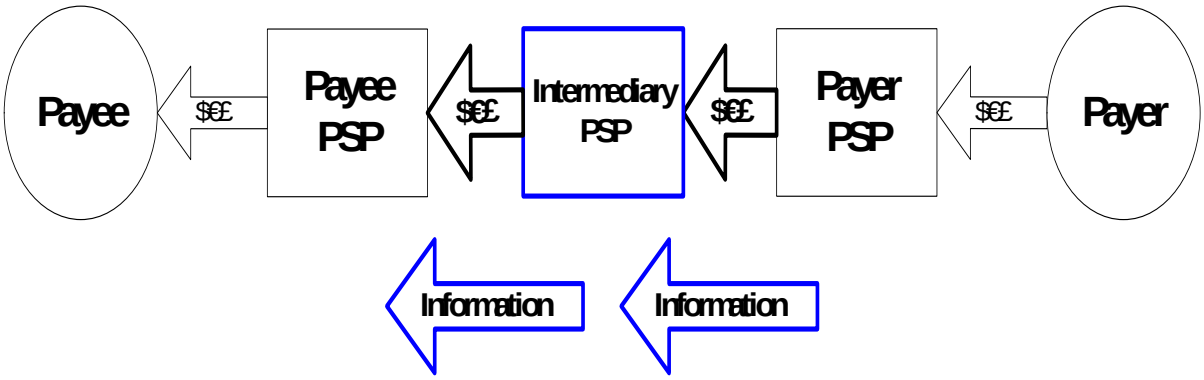
If fields regularly incomplete or information inappropriate:
- Issue warning to PSP of payer
- If no improvement, reject any further transactions or restrict / termniate business relationship
- Report to law enforcement

Note: In practice the procedures required to 'detect' may be met by a combination of system (e.g. SWIFT) validation and risk-based post event random sampling. See Part II, Specialist guidance A: *Wire Tranfers,* A.23 - 30.

Records of any information received to be kept for 5 years

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.

Scenario 3: Transfer of funds – Obligations on Intermediary PSP



Keep information received with the transfer. Where technical limitations prevent this see Part II, Specialist guidance A: *Wire Transfers*, A.18.

Where information is not sent with transfer it must be kept for 5 years

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.

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 CRED 4.3.37 G to 4.3.37J G.

This guidance applies only to FSA-regulated credit unions, not to credit unions in Northern Ireland.

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 FSA 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. There are two types of credit union, Version 1 and Version 2. The majority of credit unions are Version 1, offering very basic savings and loan products. Version 2 credit unions have much more flexibility around the products they can provide and currently just 2% of credit unions have Version 2 status. However, although Version 2 credit unions have more flexibility, in terms of the wider financial services sector both Version 1 and Version 2 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 CRED 7A.2.1 R. The return on savings is linked to financial performance and is subject to a statutory cap, currently set at 8%. In addition, there are rules governing a credit union's lending activity. Lending limits are set out in CRED 10.3.1 R to CRED 10.3.6 R.

4.6. Therefore credit union financial products, particularly those of Version 1 credit unions, 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'[5].

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

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. Examples of risks are given at www.jmlsg.org.uk but a credit union will also 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 CRED 4.3.37H G which reads, "SYSC 3.2.6H R requires a credit union to allocate to a director or senior manager (who may also be the money laundering reporting officer) overall

responsibility within the credit union 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) and, where relevant, 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 5.3.68-5.3.84), 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 5.3.74, 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. In principle, 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 5.3.39-5.3.40 and 5.3.79–5.3.81. 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 Roll check) is normally not enough on its own to verify identity.

Financial exclusion

4.18. The FSA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. The term is sometimes used in a narrower sense; for example, HM Treasury 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 5.3.68-5.3.76 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 5.3.113–5.3.114 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 person[6] 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 5.3.68–5.3.114.

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.

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

[6] 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: see www.ukpa.gov.uk/passport_countersign.asp; and others might include members of a local authority, staff of a higher or further education establishment, or a hostel manager.

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 5.3.107 and 5.3.109. 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 5.3.109.

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 5.3.107–5.3.109. 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 5.3.109.

Enhanced due diligence

4.32. There will be certain occasions when enhanced due diligence will be required, for example:

- when there is no face-to-face contact with the customer
- where the customer is a PEP
- when the person is involved in a business that is considered to present a higher risk of money laundering; examples of high risk businesses can be found at www.jmlsg.co.uk and paragraphs 1.35-1.37 of sector 1: *Retail banking*

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 SOCA. 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

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 SOCA. If he decides not to make a report to SOCA, 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 SOCA, this must be done promptly and as soon as is practicable. When a report is made to SOCA, 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 6.48-6.57) and act accordingly. Furthermore if,

under the Data Protection Act a member submits a subject access request, then the credit union should contact SOCA for advice (see Part I, paragraphs 6.84-6.93).

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 CRED 4.3.37H G 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, or references to, the evidence they obtained of a customer's identity, until five years after the end of the customer relationship
- details of customer transactions for five years from the date of the transaction
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report where 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 circumstances where it is not reasonably practicable for a credit union to copy documents used to verify identity, in any format described above, (e.g. when at a collection point) a credit union will need to keep a record of the type of document, its number, date and place of issue, as proof of identity so that, if necessary, the document may be re-obtained from its source of issue.

4.49. 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 banking and investment services in a closely managed relationship to high net worth clients. Such services will include bespoke product features tailored to a client's particular needs and may be provided from a wide range of facilities available to the client including:

- current account banking
- high value transactions
- use of sophisticated products
- non-standard investment solutions
- business conducted across different jurisdictions
- off-shore and overseas companies, trusts or personal investment vehicles

What are the money laundering risks in wealth management?

Inherent risks

5.2 Money launderers are attracted by the availability of complex products and services that operate internationally within a reputable and secure wealth management environment that is familiar with high value transactions. The following factors contribute to the increased vulnerability of wealth management:

- Wealthy and powerful clients – Such clients may be reluctant or unwilling to provide adequate documents, details and explanations. The situation is exacerbated where the client enjoys a high public profile, and where they wield political or economic power or influence.

- Multiple and complex accounts – Clients often have many accounts in more than one jurisdiction, either within the same firm or group, or with different firms.

- Cultures of confidentiality – Wealth management clients often seek reassurance that their need for confidential business will be conducted discreetly.

- Concealment – The misuse of services such as offshore trusts and the availability of structures such as shell companies helps to maintain an element of secrecy about beneficial ownership of funds.

- Countries with statutory banking secrecy – There is a culture of secrecy in certain jurisdictions, supported by local legislation, in which wealth management is available.

- Movement of funds – The transmission of funds and other assets by private clients often involve high value transactions, requiring rapid transfers to be made across accounts in different countries and regions of the world.

- The use of concentration accounts – i.e. multi-client pooled/omnibus type accounts - used to collect together funds from a variety of sources for onward transmission is 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 so as to deceive the banker.

Secured loans

5.3 Secured loans, where collateral is held in one jurisdiction and the loan is made from another, are common in wealth management. Such arrangements serve a legitimate business function and make possible certain transactions which may otherwise be unacceptable due to credit risk. Collateralised loans raise different legal issues depending on the jurisdiction of the loan. 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.

Assessment of the risk

5.4 The role of the relationship manager is particularly important to the firm in managing and controlling the money laundering or terrorist financing risks it faces. Relationship managers develop strong personal relationships with their clients, which can facilitate the collection of the necessary information to know the client's business, including knowledge of the source(s) of the client's wealth. 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 – including the temptation to put the client's interests above that of the firm
- undue influence by others

5.5 As in all firms, relationship managers and other client-facing staff 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, bankers. 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

5.6 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 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

5.7 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.

5.8 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, they should consider nominating a manager 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

5.9 In common with the provision of other financial products or services in such countries, care should be exercised to ensure that use of banking and investment services does not lead to levels of obscurity that assists those with criminal intentions. At all times care should be exercised to ensure requests for confidentiality do not lead to unwarranted levels of secrecy that suit those with criminal intentions.

5.10 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 firm.

5.11 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 client's needs will often entail the use of complex products and fiduciary services, sometimes involving more than one jurisdiction, including trusts, private investment vehicles and other company structures. Where such legal vehicles and structures are used, it is important to establish that their use is genuine and to be able to follow any chain of title to know who the beneficial owner is.

5.12 In addition to the standard identification requirement in Part I, paragraphs 5.3.68 – 5.3.78, 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
    - 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
    - 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.

5.13 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

5.14 As mentioned in Part I, paragraph 5.3.76, visiting clients can be an important part of the overall customer due diligence process. In wealth management, relationship managers should generally 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

and updating the client profile where appropriate.

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

Approval of new relationship

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

Review of client information

5.17 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)

5.18 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 not physically present for identification purposes, and those who are PEPs, see Part I, section 5.5 and paragraph 5.21 below.

5.19 Those categories 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.

5.20 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)

5.21 Firms offering a wealth management service should have particular regard to the guidance in relation to PEPs set out in Part I, paragraphs 5.5.18 to 5.5.29. 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

5.22 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.

5.23 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 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. Particular consideration should be given to the extent to which their AML/CTF legislation is comparable to the provisions of the relevant EU Directive.

Monitoring

5.24 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.

5.25 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 equivalent jurisdiction; and
- any activity not commensurate with the nature of the business.

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

5.26 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.

5.27 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.

6: Financial advisers

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.

Typical customers

6.2. The typical customers of financial advisers are personal clients (including high net worth individuals), trusts, companies. Some firms also advise 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 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 FSA 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 firm must consider the risk related to the product, as well as the risk related to the client.

6.10. Clearly, the risk of being involved in money laundering or terrorist financing will increase when dealing with certain types of customer, 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.

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.

Private individuals

6.14. Guidance on verifying the identity of private individuals is given in Part I, paragraphs 5.3.68 to 5.3.6114. Guidance on circumstances where it may be possible to use the source of funds as evidence of identity is given in Part I, paragraphs 5.3.92 to 5.3.96.

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 to be provided, 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.

Non-personal customers

6.17. Guidance on verifying the identity of non personal customers is given in Part I, paragraphs 5.3.115 to 5.3.248. Categories of non personal customers that are likely to be of particular relevance to financial advisers are:

- Private companies (paragraphs 5.3.130 to 5.3.138)
- Pension schemes (paragraphs 5.3.151 to 5.3.159)
- Charities, church bodies and places of worship (paragraphs 5.3.160 to 5.3.179)
- Other trusts, foundations and similar entities (paragraphs 5.3.180 to 5.3.202)
- Partnerships and unincorporated businesses (paragraphs 5.3.212 to 5.3.225)
- Clubs and societies (paragraphs 5.3.226 to 5.3.234)

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. 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.

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 FSA in 2005 in fining a bond broker who gave such conformation 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 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 SOCA, 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. In circumstances where a financial adviser is unable to take a record of documents used to verify identity, (e.g., when at a customer's home) he/she should keep a record of the type of document, its number, date and place of issue, as proof of identity, so that, if necessary, the document may be re-obtained from its source of issue.

6.29. 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).

6.30. 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 8.11).

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.

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, it is also recognised that although the nature of these products helps reduce the money laundering risk, the funds used to purchase them could 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:

a) The profile of the customer, including his geographical location and source of funds;
b) The delivery mechanism, or distribution channel, used to sell the product; and
c) The nature of the product being sold.

7.4 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 may add to the product risk. This is particularly the case with regard to Politically Exposed Persons – see Part 1 (5.5.18 ff). A firm must ensure that their own risk-based approach is appropriate to the particular circumstances they face.

Politically Exposed Persons (PEP)

7.5 Part 1 (5.5.18 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.

7.6 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.

7.7 Based on the experience of a number of insurers, the insurance sector has a very low exposure to PEPs. The majority of products sold by insurers also do not lend themselves to moving the proceeds of corruption. It is likely therefore that the numbers of customers meeting the high-risk criteria are very low and those that are identified as PEPs are lower still.

7.8 Firms may consider using criteria such as accounts with non-UK residents[7] and investment value to determine their risk based approach to PEP identification.

7.9 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.

7.10 The identification of a customer as a PEP is not in itself cause for suspicion, but requires an enhanced level of due diligence in line with the guidance set out in Part I. In some cases, however, this enhanced due diligence may trigger suspicions that the client is attempting to store or launder the proceeds of corruption. In such cases, a SAR and consent request must be submitted to SOCA, following the guidance set out in Part 1, chapter 6.

Distribution Risk

7.11 The distribution channel for products may alter the risk profile. For insurers the main issues will be non face-to-face sales, such as online, postal ***or*** telephone sales. Part I, paragraphs 5.5.10ff outline the process for managing non face-to-face sales.

7.12 For business sold through agencies, such as IFAs, agency acceptance and ongoing management procedures may already meet the requirements set out in Part I, paragraphs 5.6.27 and 5.6.28.. 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 breeches/financial difficulties, which might call into question the agent's status as fit and proper.

7.13 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 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

7.14 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 very different nature of each category of products (protection, pensions and investments) and the fact that each product's features are defined and restricted; some will only pay out on a verifiable event such as death or illness, whilst others are accessible only

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

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.

7.15 A smaller number of products sold by firms in the insurance sector, including single premium investment bonds and certain pensions, do feature increased flexibility. This should be acknowledged in the application of the risk-based approach.

7.16 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.

7.17 The following are features that may tend to reduce the risk profile of a product:

- 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 (eg 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.

7.18 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.

7.19 Where apparent inconsistencies exist, firms are expected to exercise judgment accordingly. For example, certain personal pension products accept contributions from an employer. Third party payments are indicative of increased risk according to the above list. Nevertheless, the other features of those pension products (the restricted access to funds, the ability to take only a percentage of the fund as a lump sum on reaching retirement age, the involvement of HMRC) together carry more weight than the fact that contributions may be received from a third party. On balance, therefore, most personal pension products remain at the lower end of the risk range (see paragraph 7.14).

7.20 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 a

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.

Three overall risk levels

7.21 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.

7.22 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.

7.23 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.

7.24 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.

7.25 Risk management is a continuous process (as noted in Part I, paragraph 4.30). The risk assessment process is not a one-time exercise, and it must be revisited and reviewed on a regular basis.

7.26 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

7.27 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 attracting Simplified Due Diligence [See Regulation 9(8)]. Others, such as Compulsory Purchase 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.

7.28 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	*Typical features:* o *Only pays out on death of assured* o *No surrender value* o *Small, regular premiums: additional payments by customer not possible* o *Large premiums will normally require medical evidence* o *No investment element* o *Once term of policy is finished no payout and policy ceases*	*Timing of verification for pure protection products* *(Part I: 5.2.2)* *ML Regs 9 (4)*
2 Income protection products related to long-term illness	o *Only pays out on medical evidence and proof required as to loss of income* o *No surrender value* o *Small, regular premiums: additional payments by customer not possible*	*Timing of verification for pure protection products* *(Part I: 5.2.2)* *ML Regs 9 (4)*
3 Critical illness products relating to diagnosis of a specific critical illness	o *Only pays out on medical evidence* o *No surrender value* o *Small, regular premiums: additional payments by customer not possible*	*Timing of verification for pure protection products* *(Part I: 5.2.2)* *ML Regs 9 (4)*
Pensions		
4 Pension, superannuation or similar schemes which provide retirement benefits to employees[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[9]	o *Long term savings vehicle* o *No surrender value* o *Product may not be used as collateral*	*Qualifies for Simplified Due Diligence* *(Part I 5.4.5)* *ML Regs 13 (7)(c)*
5 Pensions annuities, whether purchased with the company running the long-term savings vehicle or through an open market option.	o *Product already subject to due diligence and ongoing monitoring from the pension provider*	*Qualifies for Simplified Due Diligence.* *ML Regs 13(7)(b)*
6 Rebate Only Personal Pension ("RPP")	o *Only funded by National Insurance Contribution rebates payable as a result*	*Qualifies for*

[8] This would cover Contracted in and out Group Money Purchase Schemes, Final Salary Schemes, s32 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 2007 13(7)(b), and is therefore not contingent on the monetary limits set out in 13(7)(a).

	of an individual being contracted out of SERPS or S2P	*Simplified Due Diligence*
7 Immediate Vesting Personal Pension ("IVPP"). Purchased with the transfer from another pension for the purpose of exercising an open market annuity option.	o *Product already subject to due diligence and ongoing monitoring from the pension provider*	*Qualifies for Simplified Due Diligence.* *ML Regs 13(7)(b)*

Customer due diligence

7.29 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.

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

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

> Apply Simplified due diligence. Therefore *apart from monitoring,* customer due diligence does not apply to either the customer.
>
> 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, on application and with the relevant authority, HMRC will provide 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 or a visit to premises.

7.32 Where an insurer decides to apply simplified due diligence to a particular product or type of business, there is no requirement to identify or verify the identity of beneficial owners and/or controllers. Ongoing monitoring, however, is still required.

Monitoring

7.33 Companies must take a risk-based approach to monitoring reduced risk products. A company's normal anti-fraud controls should provide a suitably robust system of monitoring. The high annual limits for pensions in the post A-day tax regime provide greater scope for these products to receive large lump sum payments; a risk which may be mitigated by monitoring.

Frequently asked questions in relation to reduced risk

7.34

(i). What if, at the claim or payout stage, we identify that a third party 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 and where the firm does not consider that it has a client relationship with that person or that they are the beneficial owner (in which case the person's identity must be verified on a risk sensitive basis), there is no requirement to verify the identity of a third party payer for reduced risk products.

(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 5.3.92.

II - Intermediate risk level

7.35 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.

7.36 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	*Typical features:* o *may accrue some surrender value* o *benefits usually payable on death or diagnosis of terminal illness* o *or, in some cases, critical illness of the policyholder* o *partial surrenders are normally allowed within specified limits* o *qualifying whole of life plans will comply with the rules applicable to qualifying life policies*
Savings	
2 Life assurance savings plan	*Typical features:* o *Long term savings plan often for retirement* o *Requires at least 5 years to gain positive return on investment* o *Often unable to be surrendered in first or second year, with penalties in years three to five* o *Additional 'top up' payments may be permitted* o *Sum assured/premium relationship broadly complying with HMRC Qualifying Rules*
3 Endowments	o *Long term savings plan for a set term, were often linked to mortgages* o *Sum assured/premium relationship broadly complying with HMRC Qualifying Rules* o *Usually long term, 10-25 years*
Pensions - corporate	
4 Group Personal Pension ("GPP")	*Typical features:* o *Long term policy, usually up to 40 years* o *No surrender value* o *Pensions*
5 Group Stakeholder Plan	o *Long term policy, usually up to 40 years* o *No surrender value*

	o *HMRC registered scheme* o *Annual and lifetime limits apply*
Pensions - individual	
6 Income Drawdown Flexible Pension Plan Phased Retirement Plan	o *Typical features:* o *Policies only open to individuals between the ages 55 – 75, and people who have already accrued by a pension fund* o *The level of income which may be 'drawn down' is subject to limits set by the Government*
7 Free Standing Additional Voluntary Contribution Plan ("FSAVC")	o *Contributions cap set by pensions legislation and monitored by scheme administrator* o *Transfers are only possible to another regulated entity*
8 Stakeholder Plan	o *Long term policy, usually up to 40 years* o *No surrender value* o *HMRC registered scheme* o *Annual and lifetime limits apply*
9 Personal Pension Plan (not SIPP or SSAS)	o *Long term policy, usually up to 40 years* o *No surrender value.* o *HMRC registered scheme. Transfers are possible, but only to another registered scheme.* o *Annual and lifetime limits apply.*
10 Immediate Vesting Personal Pension ("IVPP"). Purchased for purposes other than pursuing an open market annuity option.	o *Policies only open to individuals between the ages of 50 and 75.* o *Purchase not based on a transfer from another pension scheme.* o *Annuity usually purchased with one one-off payment.*
12 Purchased Life Annuity ("PLA") Hancock Annuity	o *No return of cash lump sum at end of the term selected or when customer dies* o *Once annuity purchased, purchaser cannot alter the arrangements or cash it in.*

7.37 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

7.38 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.

7.39 In accordance with Part I, companies must identify the beneficial owner, following the guidance in Part I, paragraphs 5.3.10 and 5.3.11.

Monitoring

7.40 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. Within the post A-day pensions regime, highly atypical pensions contributions should attract higher levels of scrutiny from pensions providers.

Frequently asked questions in relation to intermediate risk

7.41

(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 SOCA 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) *Who are the relevant parties whose identity should be verified for intermediate risk pensions? What information do we need to obtain in respect of these products to satisfy customer due diligence requirements?*

For intermediate risk pensions, practically speaking the identity of anyone who pays premiums should be verified. Specifically, the parties to be verified are:

a) the employer, if premiums are paid via the employer; and
b) the employee, where contributions are also, or only, paid direct by the employee.

Terms and conditions for intermediate risk pensions will usually dictate that third party payments into the policy are prohibited. However, it is possible that payments could be made to these policies by third parties and refusing them could disadvantage the policyholder. In circumstances

where the firm is comfortable that the payments do not represent the movement of criminal funds - perhaps because the third party payment has been made by a close relative in the event of financial hardship being suffered by the policy holder or the payment being small and one off in nature - such payments can be accepted without further action. However, where such a payment was larger or more frequent in nature verification of the third party's identity would be appropriate. Where the third party payer is the customer's employer, the standard procedure for intermediate risk products would be to verify the identity of the company (but not the directors of that company).

(iv) *How does using the "source of funds" as evidence affect these intermediate risk level products?*

a. For intermediate risk level products covered by this sectoral guidance, 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 an intermediate 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 5.3.92.

c. Where use is made of source of funds as evidence, further due diligence measures are required if, subsequently, payments are made to or received from third parties. Further guidance on the use of the source of funds as evidence is given in Part I, paragraphs 5.3.92ff.

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

a. The parties to be verified are:
    1. the employer, if premiums are paid via the employer; and
    2. the employee, where contributions are also, or only, paid direct by the employee; and
    3. any third party payers.

Unless the conditions in (c) below are satisfied.

b. 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 number where relevant and the type of plan

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

    1 the transfer is **from**[10] an Occupational Pension Scheme which is not a Executive Pension Plan ("EPP") or a Small Self Administered Scheme ("SSAS"); **and**

[10] In line with the requirements of Pensions Update 132, effective from 1 July 2002, firms should place to confirm from the transferring scheme that the transfer is an approved exempt scheme.

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 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 though for small payments the firm may wish to take a view involving the risk and circumstances surrounding the transfer of the endowment policy and consider whether the use of the one off transaction exemption is appropriate. Part I, paragraph 5.3.7 provides further information on the use of this exemption. However, where there is evidence of significant or unusual trading activity, identity must be verified and further checks would also be appropriate. Where the transfer/s have taken place though a 'market maker' in traded endowments, and that firm is regulated by the FSA, reliance may be sought from the market maker in accordance with Part I, section 5.5.

In line with the requirements of Pensions Update 132, effective from 1 July 2002, firms should have adequate processes in place to confirm from the transferring scheme that the transfer is an approved exempt scheme.

(vii) *What about life assurance policies written in trust for intermediate risk products?*

Life assurance policies are commonly written as simple life trusts, usually for inheritance tax planning reasons and not for the purpose of concealing the ultimate economic beneficiary of the policy. Therefore it is not appropriate to apply the increased identity requirements recommended in Part I for trust vehicles that are used for other purposes and firms need only identify the Settlor in line with the standards in this section. However, firms should ensure that they have in place adequate procedures to identify where a trust poses a higher money laundering or terrorist financing risk.

III Increased risk level

7.42 The increased risk level has been attributed to a group of products whose inherent features open the possibility to their being used for money laundering purposes. These products may have a facility for third party and/or 'top up' payments, or are 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 these products in their respective categories of protection, savings and investments and pensions, together with the features.

7.43 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. 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	
1 Single premium investment bonds,	*Typical features:* o *Open ended investment*

including: • With profits • Guaranteed • Income • Investment • Offshore international bonds	o *Usually a 5 year recommended minimum investment term but can be surrendered earlier* o *Additional 'top up' payments permitted by policy holder and by third parties* o *May be segmented and individual segments may be assignable*
Pensions	
2 Executive Pension Plans ("EPPs") (excludes CIMPs & COMPs – see Minimal Risk section)	*Typical features:* o *Contributions from company to tax exempt fund, normally* o *Established by company directors for their benefit* o *Single premium payments permitted*
3 Small Self Administered Schemes ("SSASs")	o *Small limited companies where directors are the main shareholders* o *Flexibility of investment options* o *Able to be used to raise loan capital* o *Members can be bought out by other members of the scheme*
4 Self Invested Personal Pension ("SIPP")	o *Provides the fullest choice of allowable investments, including commercial property, i.e., can be used to buy business premises. Administered by the beneficiary.*
5 Trustee Investment Pension Plan ("TIPP")	o *Open-ended investments, money can be accessed at any time* o *Investment term can be anything upwards of 4-5 years* o *Low early surrender penalties* o *Can be linked to EPPs, SSASs or SIPPs*

7.44 As can be seen from the table above, the majority of increased risk level products are found 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. The pension products are included because of their flexibility and the capacity for large sums of money to be invested though it is recognised that the involvement of HMRC does mitigate this risk to a degree.

Customer due diligence

7.45 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)

7.46 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 5.3.10 and 5.3.11.

Monitoring

7.47 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:

7.48

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

The relevant parties are summarised in the table below:

	Relevant parties to be identified
Savings/investments	
1 Bonds	o *Policy holder or applicant* o *All payers if different to policy holder* o *All payees if different to policy holder*
Pensions	
2 EPPs	o *Employer/Trustee(s) who are beneficiaries or who may give instructions. Where trustees are: an FSA regulated financial services company then firms need obtain only the trustees' FSA regulatory number (and check it to FSA database if regulated trustee is unknown)* o *Third party payers (including the employee/policy holder)*
3 SSASs	o *Employer/Trustee(s) who are beneficiaries or who may give instruction and Pensioner Trustees who are beneficiaries or who may give instructions, to be ID verified if they do not appear on the HMRC Pensioner Trustee Approved List which is at www.hmrc.gov.uk/pensionschemes/* o *Third party payers (including the employee/policy holder)*
4 SIPPs	o *Policy holder* o *Employer (where paying premiums)* o *Third party payers*
5 TIPPs	o *Trustees (unless UK regulated financial*

	services company trustees in which case, only a confirmation of FSA regulatory number is required) o *Person giving payment instructions where a TIPP is held on behalf of a SSAS managed by another firm, unless that firm is regulated or payment can only be made to a regulated firm*

(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.

	Suggested practice for monitoring and control
Savings/investments	
1 Bonds	o *Cancellation (i.e., applications not proceeded with after funds received)* o *Early surrenders (ie within a certain time period, which is to be specified by individual firms) over a certain € threshold* o *Multiple partial surrenders, totalling up to (say) 75% of original investment, within the specified time period* o *Top up payments over a certain € threshold (dependent on individual firms' assessment of materiality) and frequency* o *Third party payments of any value* o *Non UK residents*
Pensions	
2 EPPs SSASs SIPPs TIPPs	o *Loans taken out using product as collateral* o *Top up payments when much larger than current holdings*

(ii) 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). What about increased risk level pension transfers?

a) No exemptions from identity verification requirements should be taken in respect of increased risk level pension transfers ie transfers from or to pension schemes listed as increased risk.

b) The source of funds should be identified by obtaining either via the transaction details or from the previous scheme holder or from, another trusted source:

   1. the previous pension provider's name; and

   2. the previous scheme or plan name, its reference or PSO number where relevant and the type of plan.

(vi) How does using the "source of funds" as evidence affect these 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 a Power of Attorney, the identity of the Attorney should also be verified using the principles established in Part I, paragraphs 5.3.89-5.3.91.

(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 SOCA 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.

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.

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/wrap platforms.

Typical investors using retail funds and associated products/services vary depending upon the product, but include private individuals, regulated firms investing as principal (eg. life companies); other regulated firms (including nominee company subsidiaries) acting on behalf of underlying customers, other corporates, personal and corporate 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). Nor does it cover the issue or trading of shares in closed-ended investment vehicles (eg. investment trusts). Guidance on other life assurance products can be found in sector 7: *Life assurance and life-related pensions and investment products*. The issue and trading of shares in investment trusts etc. 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.*

What are the money laundering risks relating to investment fund products?

Retail funds and products/services

8.5 The vast majority of investment fund business is conducted on a non-face-to-face basis (post, telephone, internet) and investors generally have easy access to the funds involved. In addition, some firms accept payment by debit card, which exposes them to the risk of card fraud.

8.6 However, there are also factors that limit the attractiveness of these products for any money laundering process, which therefore mitigate some of these risks. In particular, in order to mitigate the money laundering risk, firms invariably take steps to identify any third party subscribers or payees, and some firms refuse to accept or make third party payments. Furthermore, most retail investors use these products for medium and long-term savings, which makes short-term investment or high turnover unusual and often relatively straightforward to monitor.

8.7 The typical retail investor might place anything up to £50,000 in investment funds (and for ISAs investment is limited by law to a maximum of £7,000 per annum). Larger investments are not uncommon, however, especially for firms whose target market is higher net worth individuals.

8.8 Investors are rarely asked to provide additional customer information about the purpose of the relationship, which will be self-evident, or their background. However, their behaviour is better measured against that of other investors than against uncorroborated customer data, which any criminal could provide in support of their expected activity.

8.9 Holdings of investment fund units may be transferred freely between different parties. Such transfers will be recorded by the registrar of the fund (usually the product provider or a third party administrator acting on their behalf) who should have a mechanism in place to alert them to unusual transfer activity (see paragraph 8.38).

8.10 On balance, therefore, investment funds and products that involve the restrictions referred to in paragraph 8.6 may generally be considered to be low risk in terms of their use for money laundering purposes. Notwithstanding this, the firm's risk-based approach will need to take account of the additional risk that would be associated with higher value (for example, the source of funds should not be used as evidence of identity for transactions of more than £50,000 - see paragraph 8.19(ii)). In any event, if the features of a product or service provide additional flexibility (for example, where some or all of the restrictions referred to in paragraph 8.6 are not applied), the firm should consider the potential increase in the money laundering risk given all the relevant factors and, where appropriate, take additional steps to mitigate that risk (for example, by undertaking further identity verification measures and/or obtaining additional customer information). Firms should also consider whether or not the nature of their distribution channels and the geographic location of their customers might suggest that their products are more likely to be used for the purposes of money laundering.

8.11 It is accepted that those who are able to provide convincing evidence of identity and behave in the same way as other investors will be very difficult to detect, in the absence of any other information to cause the firm to have doubts about the customer. Nevertheless, whilst investment fund products may generally be unattractive vehicles for the money laundering process, firms must be alert to the fact that career criminals will almost certainly invest in their sector using the proceeds of crime, and should consider any unusual activity in that light.

Institutional funds

8.12 Many institutional funds are open only to tax-exempt investors, such as pension schemes and charities.

8.13 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 client 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.

8.14 Overall, many institutional funds may be considered to be of lower risk than their retail counterparts, albeit by virtue of the restricted types of investor, rather than the product 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.

Who is the customer for AML purposes?

8.15 The Money Laundering Regulations 2007 introduce a much wider definition of "business relationship", which now includes 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.

8.16 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.

8.17 Should a firm wish to meet a request by the investor to pay redemption proceeds to a third party, that party should likewise be regarded as a customer (on whose behalf the registered investor may have been acting), and their identity should be verified before any funds are remitted.

8.18 Firms are not required to assume that payment from an unidentified source (e.g., by wire transfer from a UK bank or building society) 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

8.19 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 exemptions and concessions are available. Typically, these would include:

(i) application of simplified due diligence in relation to qualifying customers or products as described in Part I, Chapter 5;

(ii) use of the source of funds as evidence of identity - see Part I, paragraphs 5.3.92 to 5.3.96 (firms should limit its use to lowest risk cases, and should not use it where the value exceeds £50,000).

(iii) application of the measures described in Part I, paragraphs 5.3.86 and 5.3.87 in relation to the administration of deceased investors and Court of Protection Orders.

8.20 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 in the sole or joint name of the customer.

8.21 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 5.6.18), reliance may be placed on the intermediary, following the guidance in Part I, paragraphs 5.6.19ff.

8.22 In the case of beneficial owners or controllers, unless the circumstances of the relationship indicate that more stringent measures should be undertaken (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 5.3.10 and 5.3.11).

8.23 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 5.3.151 to 5.3.159 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 allow the firm to apply simplified due diligence to such customers.

8.24 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 inevitably will have legacy customers whose identity has not been verified due to the circumstances under which they became investors, and the requirements and exemptions etc. that existed at that time. Firms 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

8.25 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, is of less relevance to this sector. 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.

8.26 Very high value transactions from individuals should, however, be treated with caution. High net worth individuals are more likely to use the services of an investment manager, who would need to obtain considerably more customer information in order to service their needs properly - direct investment by such individuals may be an indicator that they are seeking to avoid having to provide that additional information.

8.27 Furthermore, firms will need to take a risk-based approach in deciding whether or not to consider a customer's potential status as a politically exposed person (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.

8.28 The nature of retail investment products means that the reasons for using them are limited and investment will reasonably be accepted from virtually anyone wishing to do so. Furthermore, activity monitoring in this area can be equally, if not more, effective by comparing the behaviour of one customer with that of others (see paragraphs 8.35 – 8.38).

8.29 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.

Timing of verification

8.30 In this sector, 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 8.15) 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.

8.31 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).

8.32 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).

8.33 From the point at which the firm concludes it should *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) subject to (c) below, it must permit the investor to withdraw, redeem or transfer their investment upon production of the evidence of identity required by the firm;

(c) it must terminate the relationship and return any funds to the investor should they insist upon withdrawal or redemption while still refusing to produce evidence of identity, subject to considering whether or not it should make a report to SOCA and seek consent;

(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, 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

(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.

8.34 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

8.35 As mentioned in paragraph 8.28, 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).

8.36 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.

8.37 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.

8.38 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 client's custodian.

9.6 In either case, the typical firm deals with low volumes of high value customers, for which there is likely to 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 There is likely to be 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.

9.8 In most cases, all money and other assets within the portfolio are held under the control of a UK-regulated custodian, with money paid to or from the customer through their UK 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 (eg. 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, PEPs and customers from higher risk non-FATF jurisdictions, and may also be affected by 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*.

Who is the customer for AML purposes?

9.10 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.

9.11 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 client will be the other regulated firm, in which case there will be no requirement to consider any underlying beneficial ownership or control.

Customer due diligence

Verification of identity

9.12 As noted above, investment management in itself as a service would be considered as low risk. Therefore, in the absence of any features regarding the customer or service provided that are adjudged to increase that risk, standard identity verification measures, as set out in Part I, paragraphs 5.3.68 to 5.3.248, 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

9.13 The standard verification requirements for private individuals would be adequate to establish their identity, as described in Part I, paragraphs 5.3.68 – 5.3.114. The source of funds may also be used as evidence of identity (see Part I, paragraphs 5.3.92 – 5.3.96), 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

9.14 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 5.3.115 – 5.3.248.

9.16 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).

9.17 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.

9.18 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. Unless the circumstances of the relationship indicate that more stringent measures should be undertaken (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 5.3.10 and 5.3.11).

Mandates relating to third party investment vehicles

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 up 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 (eg. 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 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: *Unregulated funds.*

Timing

9.24 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. 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).

9.25 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 may terminate the relationship and return any monies received to their source. Alternatively, the firm may freeze any funds or assets pending eventual verification (see Part I, paragraph 5.2.9).

9.26 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) subject to (c) below, it must permit the investor to withdraw their investment upon production of the evidence of identity required by the firm;

(c) it must terminate the relationship and return any funds to the investor should they insist upon withdrawal while still refusing to produce evidence of identity, subject to considering whether or not it should make a report to SOCA and seek consent;

(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

(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.

9.27 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

9.28 The client take-on process for investment management customers usually involves gaining an understanding of the customer 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.

9.29 The customer information, obtained for the purposes of agreeing the firm's mandate and the ongoing management of the client'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

9.30 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.

Custody

9.31 Safe-keeping and banking services in respect of a customer's portfolio are usually provided by a custodian. Some customers, particularly institutional ones, will appoint the custodian direct, in which case the custodian will have their own AML/CTF obligations. In these cases it is the custodian, rather than the investment manager, that should consider the source or destination of any funds and whether or not an unidentified third party account is involved, provided the investment manager is not involved in instructing the custodian with regard to the receipt or payment of funds. Any account taken of information provided by the investment manager will depend upon their relationship and agreement between them.

9.32 The investment manager must consider these issues where it is itself providing safe custody, even where the activity is outsourced to a third party custodian. Arrangements will need to be made with any sub-custodian that may remit or receive funds direct for the relevant checks to be carried out and recorded on the investment manager's behalf.

Real estate transactions

9.33 Some portfolios (usually in relation to property fund vehicles or very large segregated mandates) include direct holdings in real estate. Unlike securities, the counterparties involved in the purchase and sale of direct holdings in real estate may not be other regulated financial institutions. However, such transactions are generally conducted though solicitors, and the counterparty's solicitor will be obliged to verify its client's identity.

9.34 Furthermore, 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 any reputational risk, firms may wish to seek appropriate assurances from their own solicitors that the identity of the counterparty will have been verified.

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 or investments (including investment funds). 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 customers, 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 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 IFAs, 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.

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. As there are no suitability obligations for ExO stockbrokers, firms will have little or no information about the customer. 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 equivalent 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 review 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 SOCA 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.

Leasing 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.

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 leases[11] are **outside** the scope of the ML Regulations[12]. 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.

---

[11] 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.

[12] 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.

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, 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. Direct lending motor products may also be obtained remotely without face-to-face contact; this is likely to carry a higher risk.

Customer due diligence

Dealer-introduced motor finance

11.18 In a move to reduce fraudulent credit applications, members of the Finance & Leasing Association (FLA) have subscribed to an industry standard with regard to acceptable proof of identity and the standardisation of credit application processing for face-to-face business. The procedure for customer verification involves face-to-face identity checks by the dealer, supported by subsequent validation of copy identity documents by the lender. 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).

11.20 Under the regulations dealers 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 FSA 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.

11.21 The identification of non-personal customers e.g., partnerships, companies, associations etc. should be carried out in accordance with the guidance set out in Part I, paragraphs 5.3.115ff.

Non face-to-face applications

11.22 Negotiations in respect of non face-to-face applications are normally drawn out over a period, involving vehicle specification and part exchanges, and are normally conducted over the telephone. Documentation is usually sent out by post, and the vehicles may be delivered to the customer's home. Firms should be aware that non face-to-face applications by their very nature pose a greater risk and should not, therefore, be treated as lower risk under simplified due diligence (SDD). They will therefore require identification, verification and ongoing monitoring under enhanced due diligence (refer to Part I, section 5.5), as opposed to just monitoring under simplified due diligence (SDD) rules within the current regulations.

11.23 Electronic verification may therefore be used, supported by postal communication to home address. Some lenders may seek copies of items in accordance with the procedures set out in Part I, Chapter 5.

Supervision

11.24 There are several different regulatory bodies taking responsibilities under the 2007 Money Laundering Regulations. In order to aid clarity about who supervises whom the FSA have published a flow chart that helps business to understand which regulator regulates which entities. The FSA's Money Laundering regulations pages also contain other information FSA ML regulated firms may find to be of use, including their approach to registering and supervising the businesses that fall to their responsibility. Links to this information can be found at: http://www.fsa.gov.uk/mlr. Similar documentation for OFT registered firms can be found on the OFT's website: http://www.oft.gov.uk/.

ANNEX 11-I

Industry Standard for Fraud Prevention in Credit Application Processing:

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, e.g. some leasing agreements, under the current money laundering regulations (under simplified due diligence (SDD) they no longer require identification and verification). However these standards should still be followed as they prevent fraud which is inherently tied into money laundering.

1. In credit application processing, there should be standard acceptable proofs for verification of identity and current permanent address in accordance with paragraphs 3 - 5 below. These apply in the case of:

   • new customers; and
   • current and previous customers where the proposal details show a material discrepancy from the existing account details in the records of the lender; and
   • previous customers whose last transaction expired over 12 months ago.

2. A 'material discrepancy' would include any of the following:

   • missing/wrongly spelt names;
   • change of name;
   • incorrect address information extending to post code, current or previous address;
   • incorrect time at address; and
   • conflicting employment details, bank details, date or place of birth.

3. There should be mandatory production of a full driving licence or a photo card driving licence, or a provisional driving licence with photo card, in every case bearing the customer's current address. All photo cards should be accompanied by their relevant counterpart. Where the driving licence does not bear the customer's current address, then additional proof of current permanent residence should be required (for example, by Electoral Roll confirmation).

4. In the rare circumstances where an individual cannot produce a current driving licence, the lender should verify the identity in accordance with the procedures set out in Part I, Chapter 5.

5. The driving licence should be supported, wherever possible, by at least one of the following:

   • electronic confirmation of the customer's current residence via the Electoral Roll;
   • electronic confirmation of current credit data at the current address on existing lending;
   • electronic confirmation of identity in accordance with Part I, paragraph 5.3.79

6. The waiving or variation of any of the requirements in paragraphs 1 to 5 is permissible but at the lender's own risk and discretion provided that, as a minimum, they comply with the requirements set out in Part I, Chapter 5.

Dealers

7. Payment may be made by the lender in advance of receiving copies of the evidence of identity and address, but there should be in place an arrangement to cancel the credit agreement and recover

the funds in the event that identity cannot be verified (such a payment is made by the lender at its own risk).

8. In accordance with the normal working practice of the lender concerned, identity should be satisfactorily verified in accordance with paragraphs 3 and 4 prior to authorisation being given to the dealer to release the vehicle to the customer or before settling the dealer's invoice.

9. The dealer should have sight of original documents (not copies) and should scrutinize them for authenticity and check the signature against the credit agreement. Any photographic proof of identity should also be checked for reasonable likeness of the customer.

10. The dealer should take a copy of the original proofs and this copy of the original proofs, together with confirmation that it is a copy of the original, should be submitted to the lender for subsequent document validation checks. The lender should not accept a copy of a copy.

Scope of Industry Standard

11. This Standard applies to sole traders and individuals and should be applied, wherever practical, to the main driver of the particular vehicle for a partnership or SME.

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 Regulations[13]. 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.

[13] 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.

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.

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 FSA 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 5.3.136 – 5.3.140 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 5.3.92- 5.3.96. 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 lender*s 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 5.3.115- 5.3.248. 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, paragraphs 5.3.92 – 5.3.96), 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 5.3.212-5.3.225 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.

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 The ML Regulations define who is covered by those regulations by close reference to the Third Money Laundering Directive ("the Directive"). Private equity firms in the UK are generally authorised and regulated by the FSA and are considered to be covered by the Directive and ML Regulations because they will carry on one or more of the BCD activities listed in Schedule 1 to the ML Regulations. Such firms may also be covered by the Directive and the ML Regulations because, in practice, they perform the functions of a collective investment scheme when marketing its units or shares. Private equity firms are therefore "financial institutions" within the meaning of the Directive and the ML Regulations, and reliance may be placed on them under the ML Regulations by other private equity firms and others subject to the Directive, such as banks, lawyers, accountants, etc.

13.2 Private equity business (for the purposes of this guidance) means activities relating to:

- The raising and acceptance of moneys into private equity funds (usually from institutional investors);
- The investing of these funds by providing long term finance to a range of businesses, from early stage to large established companies. Usually the investee companies are unquoted;
- The management of these investments (often involving active board participation) and exercise of negotiated equity holder rights; and
- The subsequent realisation of the investment.

13.3 Investors in private equity funds tend to have long established relationships with the private equity firm, normally resulting in a very well known investor base. Prior to making any investment in a business, the private equity firm will conduct extensive due diligence on the business identifying areas of risk, including money laundering considerations.

13.4 Once invested, ongoing monitoring of the investment through active board participation and regular involvement allows the firm to assess whether the investee's activities are consistent with the financial performance of the company, and also enables the firm to observe the conduct of the key managers of the business at first hand. In connection with investee companies, this will satisfy a firm's obligation to conduct ongoing monitoring of the business relationship under the ML Regulations.

13.5 There will always be an obligation for a firm to carry out such investigative work as it feels necessary where any circumstances exist which may lead it to suspect money laundering or terrorist financing is a risk, and the following guidance should be read in that context.

13.6 For AML/CTF purposes, in a private equity context there are two distinct groups:

- Investors in fund vehicles operated, managed or administered by private equity firms – paragraphs 13.7-13.27 (investors);

- Persons involved with the private equity firm when investing and divesting (e.g., investee companies when investing and purchasers on exit) – paragraphs 13.28 -13.50 (transactions).

Persons falling into the categories identified above may be classified by a private equity firm as its "venture capital contacts" for the purposes of other aspects of FSA regulation, as opposed to being classified as the firm's regulatory clients.

Investors

(i) Product risk

13.7 Investors typically invest in a fund as limited partners in a limited partnership. The limited partnership will usually be collectively managed or advised by the private equity firm. Investors invest for the long term and the timing of any return of capital is unpredictable. This form of investment is very illiquid, with no ready market. Transfers of interest in the partnerships can take place, but only after strict due diligence (and in some funds only after a minimum initial investment period) and usually only with the specific approval of the general partner or manager. Payments/repayments would also only tend to be made to the investor itself (any payment to a third party would usually only be made with the express consent of the general partner and/or manager of the fund).

13.8 This type of product would normally be considered to be a lower risk.

(ii) Customer risk

General

13.9 Investors in a fund are mostly institutional, such as insurance companies, pension funds of large corporates or state organisations, other financial companies and some funds of funds. There may also be a small number of high net worth individuals.

13.10 The acceptance of investors into a fund is a relatively long process with significant levels of due diligence performed by the firm and the prospective investor(s). Key representatives of the investors will often meet face to face with senior executives of the firm.

13.11 The relationship between the firm and investor is such that a high proportion of investors will often commit to consecutive funds of the firm; thus the relationship continues over a long period and source of funding remains constant.

13.12 For the reasons set out in paragraphs 13.9 to 13.11 these investors would generally be considered to be low risk, although certain high net worth individuals may require extra consideration in any risk evaluation.

13.13 Firms seeking to raise funds for the first time, or from a significantly larger investor base, may be under pressure to accept funds from potentially higher risk investors, and the extent of the due diligence should be adapted accordingly.

Timing

13.14 Identification checks in respect of investors in a fund should be completed before the fund closes. Where there is any assignment of an interest in a fund, any identification checks should be completed before the assignment is approved.

Identification

13.15 In relation to each investor a private equity firm should obtain at least the standard evidence for that type of investor in accordance with Part I, chapter 5. In most cases (see paragraph 13.16, for example), the key piece of standard evidence will be to identify whether there is any natural person beneficial owner holding an interest of 25% or more and (where there is) to take risk-based and adequate measures to verify his identity (see paragraphs 13.18 to 13.27 below).

13.16 In the case of institutional investors, it may be appropriate to conduct only simplified due diligence (see Part I, section 5.4) because the investor will itself be regulated.

13.17 Where a corporate investor is not well-known to the private equity firm and is quoted on a regulated market or exchange which is not located in the UK, the EU or in an equivalent jurisdiction, it may not be practical for the firm to obtain reliable evidence as to the quality of the regulation in that market or exchange. In addition to the standard identification requirements set out in Part I, paragraphs 5.3.127 to 5.3.130, the firm should seek to establish, where possible, who the corporate investor's external accountants, lawyers and brokers are, and their reputation in the market, before making a decision on what, if any, further verification of identity is required. Similar considerations should be made when it appears necessary to go beyond the standard evidence of identity.

Identifying the Beneficial Owner

13.18 Where the investor is a natural person or a wholly-owned investment vehicle of a natural person, it will be straightforward to identify the beneficial owner.

13.19 Where the investor is a "family office", the money will usually be provided by one or more trusts. The firm should look through the investment structure to identify the relevant trusts, and verify the trusts' identities, in accordance with Part I, paragraphs 5.3.180 – 5.3.202. 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) concerning the beneficial owners.

13.20 Where the investor is a pension fund or endowment, the firm must first understand the structure of the pension fund or endowment in order to determine its approach to identification. The 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. In identifying the beneficial owner, it is unlikely that any one individual will have an entitlement to 25% of the property (and a representation from the trustee to this effect should be sufficient).

Identifying the Beneficial Owner – Funds of Funds

13.21 It may be more complicated to identify a beneficial owner where the investor is itself a fund vehicle, including a private equity fund of funds.

13.22 The requirement to identify the beneficial owner and to understand the ownership and control structure in accordance with the ML Regulations would normally be confined to (a) the fund of funds manager or general partner (as the true "controller" of the fund of funds) (hereafter, the "Manager") and (b) the fund of funds itself. The assessment should not normally need to go beyond that part of the structure. In particular, it should not normally be necessary to keep looking "up" the structure until one or more natural persons are identified.

13.23 Where the Manager is regulated and subject to supervision in the UK, the EU or an equivalent jurisdiction, no further identification work would normally be required because the regulated Manager will usually deal as agent on behalf of the fund of funds.

13.24 Where the Manager is not from an equivalent jurisdiction, even though it may be regulated, or where the Manager is unregulated but operates in an equivalent jurisdiction (as is often the case in the US private equity industry, for example) the firm needs to exercise its judgement as to the likely risk presented by investors in the fund. Factors to take into consideration include:

- the profile of the Manager;
- its track record in the private equity industry; and
- its willingness to explain its identification procedures and provide confirmation that all underlying investors in the fund have been identified and are known to the Manager.

13.25 There will often be legitimate confidentiality concerns on the part of the Manager in respect of the beneficial owners of the fund. However, funds of funds are often widely held and it is unlikely that there will in fact be any investor which is a beneficial owner with an interest of more than 25%. Subject to the considerations in 13.24, in order to establish this, a private equity firm is entitled to rely on a representation from the manager (whether or not regulated or supervised) that, to its actual knowledge, there is no natural person beneficial owner of more than 25% of the shares, limited partnership interests or voting rights (as appropriate) in the fund of funds. Where such a natural person beneficial owner is encountered, the private equity firm must identify them and take risk-based and adequate measures to verify their identity.

13.26 In addition, the private equity firm should obtain the other items of standard evidence in relation to the Manager and the fund of funds vehicle. Depending on the results of the risk evaluation, it may be appropriate to obtain documents (for example basic constitutional documents), or a combination of documents and representations, from the Manager.

13.27 Possible examples of the sort of representations referred to in paragraph 13.25 are set out below. These representations do not represent evidence of identity in the way that the pro forma confirmations in Part I, Annex 5 do, but they should be used as part of the firm's risk-based approach and adapted accordingly.

Example of representation provided by a fund of funds manager or general partner

"We [name] [regulated by [name of regulator]] hereby certify the following in respect of [state name of fund(s) vehicles e.g. limited partnership(s)] (the "Funds"), for whom we act as agent.

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 identified the underlying beneficial owners in respect of the Funds and carried out customer due diligence on all of the investors in the Funds;
    - 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. Should we become suspicious of any such activity then, subject to any legal constraints, we shall inform [you/the relevant regulatory authorities] promptly.

3. To our actual knowledge [(having made reasonable enquiries)] there is no natural person who is the beneficial owner of more than 25% of the [shares/limited partnership interests/voting rights] in any of the Funds.

4. We will retain, until further notice, all documentation required to identify the underlying beneficial owners in respect of the Funds [and which we have obtained for the purposes of our due diligence]. [We will provide such documentation [to you][to your Compliance Officer][direct to any regulatory authority] [on request][where you are required to disclose it to such regulatory authority]]."

* Insert if provider of representation is regulated and subject to AML/CTF legislation.

Transactions

(i) Product risk

13.28 The product is the provision of funds by the firm in a number of different structures predominantly to unquoted companies. The funding is usually provided for the long term, after the company and its management have been subject to detailed due diligence and investigation. The firm has an ongoing obligation to monitor its investment, often involving representation on the board of the company and receipt of regular financial and operational information.

13.29 The shareholding is highly visible and any failings on the part of the company would be closely aligned to the reputation of the private equity firm.

13.30 If all these factors are present it is considered unlikely the provision of funding will be used for illegal purposes and that therefore the product will be a lower risk. The absence of one of these factors, such as the non availability of detailed due diligence work or the reliance on a third party, may require the firm to obtain more detailed verification to satisfy itself that the funds are being provided for legitimate purposes.

(ii) Customer risk

13.31 There are a number of parties involved in a private equity transaction, and the level of identification required in respect of each will vary.

Investee company (company into which funds are being paid) and its directors

13.32 All directors should be identified and the identity of key directors should be verified in accordance with Part I, paragraph 5.3.142.

13.33 This company will either have been the subject of extensive due diligence, or will be an "off the shelf" vehicle, especially established by the firm for the purpose of acquiring the investee company. Where the firm or the fund it manages, is acquiring securities in the investee company direct from a shareholder, the guidance in paragraphs 13.49 and 13.50 is relevant.

13.34 The jurisdiction of the vehicle may cause the risk profile of the investee company to increase, but provided that the company has been properly established and that the reason for the selection of jurisdiction is understood and appropriate, there should be no need to obtain additional verification.

13.35 Whilst the legal obligation relates to identifying the investee company into which funds are being paid, where that vehicle is itself undertaking a linked transaction there must be a clear understanding of the ultimate recipient of the funds and the flow of financing, particularly with the increasing complexity of deal structures.

Relevant Co-investor

13.36 Where the firm acts as lead investor in the round of financing where it has arranged co-investors' involvement in the deal, and where the co-investors are relying on the firm, it must identify the co-investors.

13.37 Following the firm's assessment of the overall risk presented by those co-investors, it may decide to verify their identity.

13.38 The identification requirements exist not only at the initial investment stage but also at any follow-on financing, to the extent that any new relevant co-investors are taking part. The firm should understand the business of a new co-investor and the reasons for it wanting to invest, particularly when the target of the financing is not performing well.

Timing

13.39 Customer due diligence checks should usually be completed when it is reasonably certain that the deal will complete, and in all cases before completion of the investment. Where there are subsequent changes to the board of directors, consideration should be given to the need to verify the identity of the new directors in light of the guidance in paragraph 13.32.

Purchaser on exit

13.40 The realisation of a private equity transaction will typically be made either by means of a listing, to a trade buyer, to existing management or to another private equity fund. If the sale is to a member of existing management who has been known to the private equity firm in the context of

the investment concerned (or of another investment), the firm should consider the relevance of any verification given its existing relationship with, and knowledge about, the management.

13.41 The pressures of achieving a successful exit may heighten the risk of limiting the amount of due diligence performed on any potential purchaser on exit. In these circumstances the firm needs to ensure that its controls for proper verification of identity and source of funding remain robust. Where the purchaser is a private equity fund, consideration should be given to a risk-based approach of the kind described in relation to fund of fund investors into a private equity fund (see paragraphs 13.21 to 13.27 above). This will often be appropriate.

Timing

13.42 Identification checks should usually be completed on purchasers of an existing investment as soon as practicable when a deal looks reasonably likely to proceed and in all cases before completion of the sale.

(iii) Market risk

13.43 The range of companies invested in is determined by the stated parameters of the fund as agreed with the investors and the level of regulation and standard of controls in which each operates will vary enormously. The strength of the firm's due diligence process serves to identify where any risk exists within the investee companies and the firm should develop its AML/CTF approach accordingly.

13.44 Providing funding to a company which operates across a number of unregulated territories, even if the parent is incorporated or registered in a well-regulated territory, may be a higher risk than an equivalent business which operates out of one well-regulated territory, and appropriate levels of verification should be considered.

13.45 An assessment may be required as to whether the type of business being invested in is likely to be a target for money launderers, and the approach to due diligence adapted accordingly. Businesses which involve high volumes of cash or near cash transactions, for example, casinos, hotels, are likely to be at greater risk than, for example, an early stage biotech company.

(iv) Other issues

Representations issued by private equity firms to third parties

13.46 In respect of their Funds, firms should be prepared to confirm whether to their actual knowledge there is any natural person who is the beneficial owner with an interest exceeding 25% of that fund. When disclosing information about investors in accordance with relevant confidentiality provisions, firms should consider agreeing to disclose the information to a certain officer or department within the third party, such as the Compliance Officer only.

Use of verification carried out by others

13.47 Private equity firms make extensive use of professional advisers, especially where the required knowledge does not exist in the firm itself. The investee companies themselves 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 an equivalent jurisdiction,

to verify the identity of their clients. Depending on the circumstances, and the firm's knowledge of/relationship with the investee company, the firm may consider it appropriate to take account of information or written assurances provided to the firm by these third parties, as part of the overall risk-based approach.

13.48 The requirement to appear before a notary in certain jurisdictions when signing documents such as the purchase contract, shareholder's agreement etc, 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.

Vendor (beneficiary of funding decision)

13.49 The decision to invest by the private equity firm will usually result in one or more individuals benefiting financially. In some instances these individuals will continue to be shareholders in the company, with the benefit being represented by the potential of significant future gains. In other cases, the beneficiary(ies) may be the original founders of the business who no longer participate.

13.50 The firm will not wish to damage its reputation by becoming associated with inappropriate individuals. Whilst vendors of an investee company are not customers of the firm under the ML Regulations unless they are selling securities in the investee company directly to the firm or to its fund(s), the firm should be aware of who the vendors are. The nature of the due diligence work performed is such that the origins of the business and the individuals involved will have been the subject of extensive review and investigation. It should ensure that it has sufficient information about the vendors (this may or may not require obtaining verification of identity) so as to be able to demonstrate that the firm had no knowledge or reasonable grounds for suspicion of money laundering on the part of any vendors in relation to the transaction.

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:

(i) 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;

(ii) 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;

(iii) C*hanges in the ownership of a business.* Examples include: advising on mergers and takeovers, or working with a company to find a strategic investor;

(iv) B*usiness 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.

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 as to the source and nature of the funds or assets involved in the transaction.

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.

Purchaser of securities

14.10. 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* in new issues 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 (which will have a customer relationship for AML purposes with the purchaser).

14.11. To protect its own reputation and that of the issuer, a firm that is acting as arranger in the issue of securities may wish to ensure that appropriate investor identification measures are adopted in the offering and that the entity administering the subscription arrangements understands the legal and regulatory AML requirements and confirms to the firm that it will undertake appropriate customer due diligence on its customers participating in the purchase of securities.

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 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-senstive 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 equivalent 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 is issued or an engagement letter is signed is the point at which the firm enters into a formal relationship with the customer. However, it is common for a firm to begin discussions with a customer before a mandate or engagement letter has been signed.

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, but this must be before the establishment of a business relationship. In all cases, however, the firm must ensure that it has completed appropriate customer due diligence prior to entering into a legally binding agreement with the customer to undertake the corporate finance activity.

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 satisfy 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

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 5.3.68 to 5.3.248 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 5.3.70. 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.

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, and staff using their knowledge of the customer, and what would be normal in the given set of circumstances, to be able 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.

Staff awareness, training and alertness

14.42 The firm must train staff on how corporate 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 corporate finance transactions and should be tailored around the specific risks that this type of business represents. Whilst there is no single solution when determining how to deliver training, training of relationship management staff via workshops may well prove to be more successful than on-line learning or videos/CDs.

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 Notes.

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

Overview of the sector

15.1 The term 'Trade Finance' is used to describe various operations, usually but not exclusively undertaken to facilitate trade or commerce. Such operations comprise a mix of money transmission instruments, default undertakings and provision of finance and are described in more detail below. Trade Finance operations are often considered in a cross-border context but can also relate to domestic trade. In volume terms the majority of Trade Finance operations are of a routine nature. Nevertheless, it is recommended that firms create a risk policy appropriate to their business which they may be required to justify to their regulators.

15.2 The three 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/instruments, rather than automatically assuming that they fit into a particular category simply because of the name that they may have been given.

15.3 There is sometimes no specific dividing line between either the categories of Trade Finance outlined below or when a lending facility is generic or Trade Finance specific. Firms are, therefore, strongly encouraged to consider the nature of the transactions they are handling.

Funds Transmission/Payments

15.4 Trade Finance operations often involve solely transmission of funds where the payment is subject to presentation of document(s) and/or compliance with specified condition(s). Typical instruments which come into this category are Letters of Credit and Collections. Financing may on occasion be provided either specifically related to the instrument itself, or as part of a general line of credit.

Default Undertakings

15.5 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.

15.6 Structured Financing

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).

Glossary of trade finance terms used in this guidance

15.7 *Bills of Exchange*. A signed written 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. 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.

15.8 *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.

15.9 *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).

15.10 *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.

15.11 *Documentary Credits*. Historically, these were one of the most commonly used instruments in Trade Finance transactions but their usage has declined in recent years, particularly in intra-Western European trade. They are, however, still used extensively 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 (UCP 600 superseded UCP 500 on 1 July 2007).

15.12 *Collections*. A typical documentary collection involves documents forwarded by an exporter, or the 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 other contexts. However, Collections of the type described above are normally but not always handled subject to the applicable ICC Rules for Collections - URC in force (currently ICC Publication 522).

15.13 *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.

15.14 *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.

15.15 *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". Mere examination of the documents without giving of value does not constitute a negotiation.

15.16 *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). There is an active secondary market for forfaiting paper.

What are the money laundering/terrorist financing risks in Trade Finance?

15.17 Globally a substantial volume of routine Trade Finance transactions take place each week. 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.

15.18 FATF's June 2006 study of Trade Based Money Laundering defined this as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize 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.

15.19 A firm's risk-based approach should be designed to ensure that it places an emphasis on deterring, detecting and disclosing in the areas of greatest perceived vulnerability. In this context, regard should be had to the fact that the majority of Trade Finance transactions take place in modest-value volume businesses, and relatively few in specialised, or otherwise high value business areas.

15.20 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. 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.

15.21 Trade Finance is generally used instead of clean payments and generic lending 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 money at some point.

15.22 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.

Assessing the money laundering/terrorist financing risk

15.23 The ability of a firm to assess the money laundering or 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.

15.24 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 firm's business mix.

15.25 FATF's June 2006 study notes that the basic techniques of trade-based money laundering include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely describing goods and services.

Firms need to be aware of these 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 report which are reproduced in Annex 15-II.

Customer due diligence

15.26 Firms must be aware of their obligations under POCA, which cannot be compromised or qualified when using a risk-based approach. Subject to the foregoing, as part of their risk policy and assessment firms should be mindful of the need to balance the risk of incurring civil claims for breach of contract when the correct documents have been presented, and their obligations under POCA.

15.27 With the partial exception of Inward Collections (see below) appropriate and acceptable 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 specifically on enquiry.

15.28 It should be noted that the instructing party will not necessarily be an existing customer of the firm and, if not, due diligence must be undertaken on the instructing party before proceeding with the transaction.

15.29 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:

- Import (Outward) Letters of Credit - the instructing party for the issuing bank is the applicant.
- Export (Inward) Letters of Credit - the instructing party for the advising/confirming bank is the issuing bank.
- Outward Collections - the instructing party is the customer/applicant.
- Inward Collections - due diligence should normally be undertaken on the instructing party but where this is not practical may exceptionally be undertaken on the drawee.
- Bonds/Guarantees - the instructing party may be either a customer, correspondent bank or other third party.

15.30 *Forfaiting* - 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.

15.31 In the primary Forfaiting, or origination, market, a firm will usually be dealing directly with an exporter, who will be its customer and who should undergo 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 and depth of scrutiny will depend on the firm’s risk assessment of the client and transaction.

15.32 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.

15.33 *Structured Financing* – As stated in paragraph 15.2, 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.

Additional due diligence

15.34 Where a firm's risk policy determines that additional due diligence is appropriate, some of the checks firms could undertake (not all of which may be applicable in each case) include:

- make enquiries as appropriate into the ownership and background of the instructing party or the beneficiary of the transaction, taking further steps to verify information or the identity of key individuals as the case demands;
- build up a record of the pattern of a customer's (i.e., the instructing party's) business, to facilitate identification of unusual transactions;
- check the transaction against warning notices from ICC's International Maritime Bureau;
- refer the transaction to ICC Commercial Crime Services for bill of lading, shipping and pricing checks;
- 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.

Monitoring

15.35 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.

15.36 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.

Staff awareness, training and alertness

15.37 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. Whilst there is no single solution when determining how to deliver training,

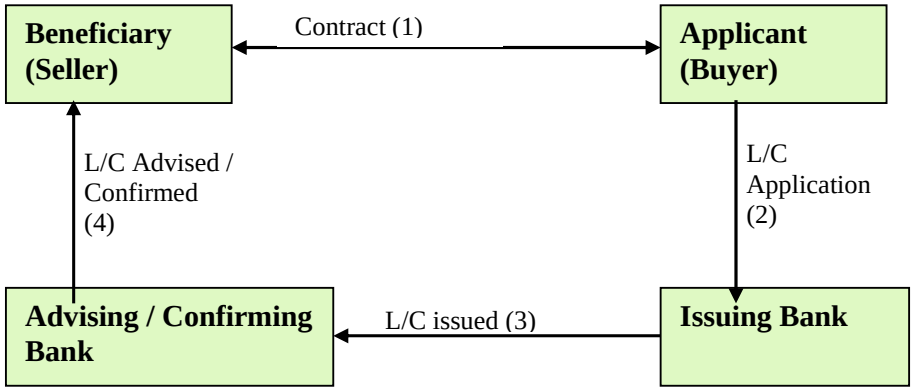
training of relationship management staff via workshops may well prove to be more successful than on-line learning or videos/CDs.

15.38 The FATF's red flag indicators set out in Annex 15-II, 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. This study is available at www.fatf-gafi.org/dataoecd/60/25/37038272.pdf

ANNEX 15-I

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

Stage 1



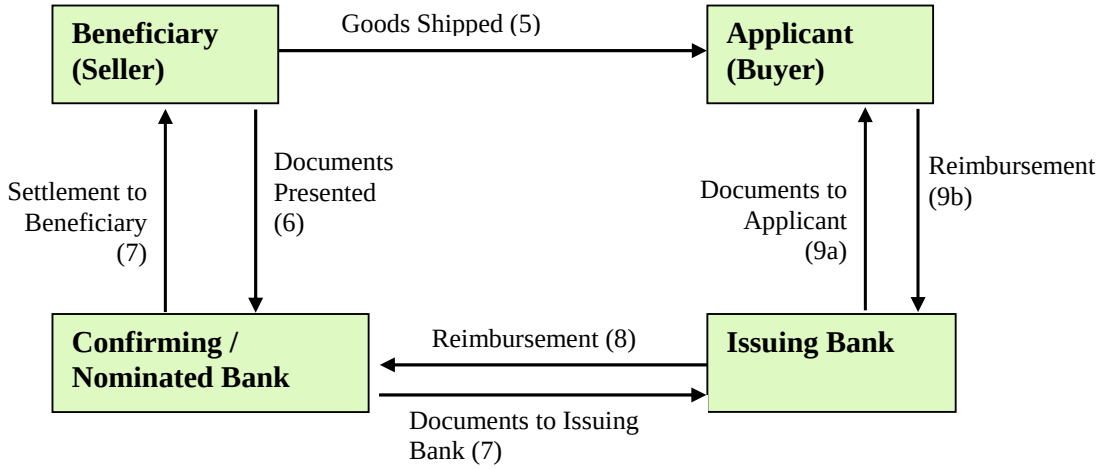
1. The Applicant (buyer) and the Beneficiary (seller) agree a sales contract, which provides for payment through a documentary credit.

2. The Applicant then requests his bank, the Issuing Bank, to issue a documentary credit in favour of the Beneficiary. The Issuing Bank, in so doing, is giving its irrevocable undertaking to make payment to the Beneficiary provided that the Beneficiary complies with the terms and conditions of the documentary credit.

3. The documentary credit is advised to the Beneficiary through a bank in the exporter's country (the Advising Bank).

4. The Advising Bank advises the documentary credit to the Beneficiary, and in this example, also adds its confirmation to the credit (becoming the Confirming Bank). A confirmed documentary credit carries the additional undertaking of the Confirming Bank.

Stage 2



5. The Beneficiary ships the goods to the Applicant.

6. The Beneficiary then prepares and presents the documents required under the documentary credit to the bank nominated in the credit as the paying bank, which in this example, is also the Confirming Bank.

7. The documents are checked against the terms and conditions of the documentary credit, and, if they are in order, settlement is effected to the Beneficiary and the documents are forwarded by the Confirming Bank to the Issuing Bank.

8. When the Issuing Bank has checked the documents and found them in order, it will reimburse the Confirming /Paying Bank in accordance with the arrangement between the two banks.

9. The documents will then be released to the Applicant against payment or on other terms arranged between the Issuing Bank and the Applicant.

ANNEX 15-II

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.
- 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.

16: Correspondent 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.

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 should take into account when considering applying a risk-based approach.

Overview of the sector

16.1 For the purposes of this guidance, correspondent banking is defined as the provision of banking-related services by one bank (Correspondent) to an overseas 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.

16.2 Correspondent banking activity can include establishing accounts, exchanging methods of authentication of instructions (e.g. by exchanging SWIFT or telex test keys and/or authorised signatures) and providing payment or other clearing-related services. A correspondent relationship can be based solely on the exchange of test keys, with cover for direct payment instructions being arranged through a third bank for credit to the Correspondent's/Respondent's own account in another jurisdiction. Activity can also encompass trade-related business and treasury/money market activities, for which the transactions can be settled through the correspondent relationship. 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. Credit, operational and reputational risks also need to be considered.

16.3 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.

What are the money laundering risks in correspondent banking?

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. For these reasons, correspondent banking is in the main non face-to-face business and must be regarded as high risk from a money laundering and/or terrorist financing perspective. Firms undertaking such business are required by the ML Regulations (Regulation 10) "to apply on a risk-sensitive basis enhanced customer due diligence measures". These requirements are addressed in this guidance.

16.5 Correspondent banking relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CTF systems and controls direct access to international banking systems.

16.6 A Correspondent handling transactions which represent the proceeds of criminal activity or terrorist financing risks regulatory fines and/or damage to its reputation.

How to assess the elements of risk in correspondent banking

16.7 For any Correspondent, the highest risk Respondents are those that:

- 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.

16.8 Correspondents must not maintain relationships with Respondents that are shell banks (see Part I, paragraphs 5.3.65 – 5.3.67) nor any Respondent which provides banking services to shell banks.

16.9 Enhanced customer due diligence (see Part I, section 5.5) must be undertaken on Respondents (and/or third parties authorised exceptionally to provide instructions to the Correspondent e.g., other entities within a Respondent group) using a risk-based approach. 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:

- **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, 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.

- **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.

Customer due diligence

16.10 All correspondent banking relationships with Respondents from non-EEA states must be subject to an appropriate level of due diligence which as a minimum meets the requirements laid down in Regulation 14 (3) of the ML Regulations and additionally will ensure that a Correspondent is comfortable conducting business with/for a particular Respondent (and hence its underlying customers) given the Respondent's risk profile. It may be appropriate for a Correspondent to take some comfort from the fact that a Respondent domiciled in 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 Correspondent may choose to rely on publicly available information obtained either from the Respondent itself, another reputable existing Respondent, from other credible sources (e.g., regulators, exchanges), or from reputable information sources, to satisfy its due diligence requirements.

16.11 The extent of the correspondent relationship should be factored into the level of due diligence undertaken. A Correspondent, subject to its risk-based approach, may decide not to undertake more than the minimum level of due diligence set out in Regulation 14 (3) for limited correspondent relationships, such as the exchange of test keys.

16.12 The verification of identity of Respondents should be undertaken in accordance with Part I, Chapter 5. Their ownership structures should be ascertained and understood and, for those privately-owned Respondents where it is appropriate to identify significant owners and/or controllers (beneficial owners), the form of evidence and information gathered on such owners and controllers must be sufficient, on a cumulative basis, to confirm identity with reasonable certainty.

16.13 A Correspondent's policies and procedures should require that the information, including due diligence, held relating to a Respondent is periodically reviewed and updated. The frequency of review should be tailored to the perceived risks, 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.

16.14 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.

16.15 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 16.9) 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 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 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.

- **Shell banks.** Whether the Respondent has confirmed that it will not provide banking services to or engage in business with, shell banks.

16.16 Prior to establishing a new correspondent relationship a person from senior management and independent from, the officer sponsoring the relationship must approve the setting up of the Respondent's account. For higher risk relationships, the Correspondent's compliance (or MLRO) function should also satisfy itself that the risks are acceptable.

Enhanced due diligence

16.17 Correspondents are required by Regulation 14(3) of the ML Regulations to subject Respondents from non-EEA States to enhanced customer due diligence, but should consider doing so whenever the Respondent has been considered to present a greater money laundering/terrorist financing risk. The enhanced due diligence process 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 well as recent material ownership changes (e.g. in the last three years). Similarly, a more detailed understanding of the experience of each member of executive management as well as recent material changes in the executive management structure (e.g., within the last three years).

- **Respondent's business.** Gather sufficient information about the Respondent to understand fully the nature of its business. In addition, determine from publicly-available information the reputation of the Respondent and the quality of its supervision.

- **PEP involvement.** If a PEP (see Part I, paragraphs 5.5.18-5.5.29) 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.

- **Respondent's anti-money laundering/terrorist financing controls.** An assessment of the quality of the Respondent's AML/CTF and customer identification controls, including whether these controls meet internationally recognised standards. The extent to which a Correspondent should enquire will depend upon the perceived risks. 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.

- **Document the relationship.** Document the respective responsibilities of the Respondent and Correspondent.

- **Customers with direct access to accounts of the Correspondent.** Be satisfied that, in respect of these customers, the Respondent:
  - (i) has verified the identity of, and performs ongoing due diligence on, such customers; and
  - (ii) is able upon request to provide relevant customer due diligence data to the Correspondent.

Monitoring

16.18 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.

16.19 The level of monitoring activity undertaken by a Correspondent on its Respondent's activity through it should be commensurate with the risks posed by the Respondent. Due to the significant volumes that correspondent banking activity can entail, electronic monitoring processes are often the norm.

16.20 The following possible techniques of monitoring activity combine to represent electronic monitoring good practice in the area of correspondent banking relationships:

- <u>Anomalies in behaviour</u>
  - Monitoring for sudden and/or significant changes in transaction activity by value or volume.

- <u>Hidden relationships</u>
  - 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.

- <u>High risk geographies and entities</u>
  - 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.

Other monitoring activity

16.21 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.

16.22 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.

16.23 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.

16.24 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

16.25 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. Whilst there is no single solution when determining how to deliver training, training of relationship management staff via workshops may well prove to be more successful than on-line learning or videos/CDs.

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.

17.2 The following sets out the relationships that exist 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, which may include:
    - 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 to provide financial information); and
    - 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).

- **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 equivalent 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.

Primary market for syndicated loans

Who is the customer for AML purposes?

17.8 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

17.9 The mandated Lead Manager/Arranger/Bookrunner should apply the guidance set out in Part I, Chapter 5, and in particular, the guidance on reliance on third parties in Part I, section 5.6, in line with the firm's risk-based approach, to the Borrower and to the Agent.

17.10 The Agent should apply the guidance set out in Part I, Chapter 5, (and in particular, the guidance on reliance on third parties in Part 1, section 5.6) 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, (and the mandated Lead Manager qualifies as a "third party" under the ML Regulations) may take account of, or rely on, 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.

17.11 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, or relying on, the due diligence carried out by the mandated Lead Manager/Arranger/Bookrunner on the Borrower.

17.12 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, or rely on, the due diligence carried out by the mandated Lead Manager/Arranger/Bookrunner and/or Agent on the Borrower where they are in an equivalent jurisdiction.

17.13 Where the Borrower has provided a Guarantor as part of the loan agreement, all parties who have an obligation to identify the Borrower - mandated Lead Manager/Arranger/Bookrunner, Lenders and Agent - should consider whether it is necessary, based upon their risk-based approach, to apply to the Guarantor the verification procedures they are applying to the Borrower.

17.14 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.

17.15 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 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

17.16 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.

17.17 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

17.18 A firm selling 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 purchaser.

17.19 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.

17.20 The money flows are 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 to verifying the identity of the Borrower, in accordance with the guidance set out in Part I, Chapter 5.

17.21 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.

17.22 In addition, a firm purchasing a loan in the secondary market must check the underlying Borrower against the HM Treasury Consolidated List.

17.23 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:

- 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 the HM Treasury Consolidated List.

Monitoring

17.24 The money laundering risks for firms undertaking syndicated lending activities can be mitigated by implementing appropriate documented monitoring procedures. General guidance on monitoring is set out in Part 1, section 5.7.

17.25 The level of monitoring to be undertaken by a firm must be commensurate with the risks posed by the Borrower. In general, the type of customer entering into syndicated loan arrangements can be regarded as low risk, but extra care needs to be taken when dealing with organisations outside the normal customer profile, for example, private companies.

17.26 There needs to be a mechanism for monitoring any variations in the loan arrangements, for example accelerated repayments, or early redemptions without good commercial rationale. This will require clear documentation of when receipts are normally due and a means of checking against this. Variations clearly need to be reported to management so that appropriate enquiries can be made.

17.27 It will also be necessary to monitor for changes in the nature and status of the Borrower. This should entail checking the information about the Borrower on a periodic basis and also any external factors which could result in a material change in the risk profile of the Borrower.

Staff awareness, training and alertness

17.28 General guidance on staff awareness, training and alertness is set out in Part 1, Chapter 7. As syndicated lending activities for the most part are considered to be low risk, the general guidance in Part I may be considered sufficient to meet the firm's needs. However, it is important for the firm to consider how syndicated lending activities may be used for ML/TF purposes and to train staff accordingly, and to train staff in the firm's procedures for managing this risk. Whilst there is no single solution when determining how to deliver training, training of customer relationship management staff via workshops may well prove to be more successful than on-line learning or videos/CDs.

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 19: *Name Passing Brokers*, which is directed at those firms who deal with wholesale market brokers in the inter-professional markets.
- Sector 20: *Unregulated Funds*, which is intended for firms who provide services, including the execution and clearing of transaction in wholesale market products, to unregulated funds.

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 Traded products confer 'rights' or 'obligations'; either between an investor and the issuer, or between parties engaged in the trading of the instruments. Traded product instruments can be bought, sold, borrowed or lent; as such, they facilitate the transfer of property or assets and usually represent 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).

18.3 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.

Exchange-traded products

18.4 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 (for their own account) or as agent for the firms' underlying customers.

18.5 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 (see paragraphs 18.48ff). Similar relationships may be recognised on other exchanges and different terminology used to denote these relationships

OTC products

18.6 OTC products are bilateral agreements between two parties, or multilateral, 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 OTC clearing facilities.

What are the money laundering risks in the wholesale markets sector?

18.7 Traded products are usually traded on regulated markets, or between regulated parties, or with regulated parties involved acting as agent or principal.

18.8 However, the characteristics of products that facilitate the rapid, and sometimes opaque, transfer of ownership, the ability to change the nature of an asset, and market mechanisms that potentially extend the audit trail, together with a diverse international customer base, have specific money laundering risks that need to be addressed and managed appropriately.

18.9 One of the most significant risks associated with the wholesale markets and traded products, is where a transaction involves payment in cash and/or third party payments.

18.10 Firms dealing in traded products in the wholesale markets are not as likely to be used in the placement stage of money laundering as, for example, deposit takers. That said, given the global flows of funds in the wholesale financial markets, it is important to recognise that although customers may remit funds from credit institutions, a firm could still be targeted with respect to the layering and integration stages of money laundering. Traded products might, for example, be used as a means of changing assets rapidly into different form, possibly using multiple brokers to disguise total wealth and ultimate origin of the funds or assets, or as savings and investment vehicles for money launderers and other criminals.

18.11 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. In the money markets, however, customers may request payments to third parties (e.g., FX payments to suppliers) and the associated AML risks need to be considered by the firm (see paragraph 18.15ff). There may also be third party funding of the transactions in the commodities

markets. Also, where a bank is lending 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 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.

18.12 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 their risk-based approach, when identifying the customer and determining appropriate payment procedures.

18.13 OTC and exchange-based trading can also present very different money laundering risk profiles. Most exchanges are regulated, transparent, and cleared by a central counterparty, and thus can largely be seen as carrying a lower generic money laundering risk. OTC business may, generally, be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. When dealing in the OTC markets firms will, therefore, need to take a more considered risk-based approach, and undertake more detailed risk-based assessment.

18.14 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.

How to assess the elements of risk in the wholesale markets sector

Generic risk elements

18.15 The main factors to consider when assessing the risk when undertaking business in the wholesale markets are the nature of the customer (including their source of funds), the market participants, the products involved and whether the products are exchange traded or OTC.

18.16 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 firms might 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 firms present might typically include, but not be 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);
    - Trust and partnerships.
- A customer's nature, status, and the degree of independent oversight it is subject to, will affect the firm's assessment of risk for a particular customer or 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 his reasons for trading, will help inform decisions on the risk profile they present.

- The way that a firm addresses the jurisdictional risk posed by a customer will depend on many factors. The jurisdictional risk may, however, 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. 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, although a firm should consider other risks, such as corruption.

- 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.

Wholesale market sub-sectors

18.17 The risks set out above are, largely, securities focused, but equally apply across the wholesale markets. The following sections look at particular risks associated with other sub-sectors within the wholesale markets.

Foreign exchange

18.18 To the extent that firms dealing in foreign exchange (FX) in the wholesale market tend to be regulated financial institutions and large corporates, the money laundering risk may be viewed as generally lower. However, this risk may be increased by the nature of the customer, or where, for example

- high risk clients (including PEPs) undertake speculative trading; and/or
- requests are made for payments to be made to third parties: for example, customers, particularly corporates, that need to make FX payments to suppliers and overseas affiliates.

18.19 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.

18.20 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 AML checks.

Financial derivatives

18.21 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 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.

18.22 The risks between exchange-traded derivatives and OTC derivative products in the financial derivative markets are the same as those set out in paragraphs 18.7 – 18.14.

Commodities

18.23 Where a customer deals purely in physical commodities for commercial purposes, the activity is not captured by the ML Regulations. 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, however, be subject to the ML Regulations, including due diligence requirements with regard to that customer.

18.24 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 might 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 firm present 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;
  - 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.

18.25 The risks should be taken in the round, with one risk possibly mitigating another. 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.

Structured products

18.26 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).

18.27 There is a wide range of users of structured products. Typically they will include:

- Corporates,
- Private banks,
- Government agencies,

- Financial institutions

18.28 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. In these circumstances it is important to clarify where the customer relationships lie and to set out each party's responsibilities in relation to identification and verification obligations.

18.29 Because of the sometimes complex nature of the products, they may generally be more difficult to value than cash securities. The lack of transparency may make it easier for money launderers, for example, to disguise the true value of their investments.

18.30 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 to determine the money laundering risk inherent in the structures.

18.31 The cash movements 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 structured products is part of a wider business relationship, and is compatible with other activity between the firm and the customer, the risk may be reduced.

Who is the customer for AML purposes?

18.32 It is very important to distinguish the relationship that exists between the various parties associated with a transaction. In particular, the firm should be clear whether it is acting as agent or principal on behalf of the customer, and whether the firm has a responsibility to verify the identity of any underlying customers involved in transactions.

18.33 Where the firm's customer qualifies for the treatment of simplified due diligence (see Part I, section 5.4), no customer due diligence is required. This would be true even where the firm is aware that its customer is acting on behalf of an underlying customer who would not itself qualify for simplified due diligence; no question of reliance under Regulation 17 will arise.

18.34 Therefore, from an AML/CTF perspective:

- If the firm is acting as principal with another exchange member, that party is the firm's customer.

- 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 employ a common or central counterparty to match and settle the trades, the firm cannot know and therefore does not need to verify the identity of 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 the firm is acting as agent for in the transaction.

- Where a firm is acting as principal with a non-exchange member, the non-exchange member is the customer of the firm.

- Where a firm is acting directly on behalf of another party (e.g., as agent), the party for whom the firm is acting will be the firm's customer.

- Where the firm is acting for another party who is itself acting as agent for its underlying customers, the following should apply:

    - The agent is the customer, not the underlying principal (who is a beneficial owner).
    - Where simplified due diligence can be applied to the agent (see Part I, Chapter 5, section 5.4) there is no requirement to identify underlying principals, unless otherwise agreed by the parties.
    - Where the agent is unregulated or regulated within a non-equivalent jurisdiction, both the agent and the underlying principal will be considered to be customers for AML/CTF purposes.

Other considerations

18.35 In certain markets there are other types of relationship associated with a transaction that are not covered under an agent or principal relationship, and these should be subject to other considerations by a firm when considering what is appropriate customer due diligence.

Different types of customer relationship

(a) Introducing brokers/Receivers and Transmitters of orders

18.36 As the name implies, 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.

18.37 As such, the customer being introduced is a customer of both the introducing broker and the firm.

(b) Executing brokers and clearing brokers in the exchange traded markets

18.38 Customers wishing to execute transactions on certain regulated markets may do so through a "give-up agreement" whereby the customer elects to execute transactions through one or more executing brokers and to clear the transaction through a separate clearing broker. Once the transaction is executed, the executing broker will then "give-up" that transaction to the clearing broker for it to be cleared through the relevant exchange or clearing house.

18.39 Both the executing broker and the clearing broker have a relationship with the customer (e.g., both may be agents), for whom they perform separate functions.

18.40 It is usually (but not always) the customer that elects to execute transactions through one or more brokers and to clear such transactions through another broker and, to that end, selects both the clearing broker and executing broker(s).

18.41 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 customers, they, too, may be customers for AML/CTF purposes (see paragraphs 18.32 – 18.34).

18.42 Where a firm acts as clearing broker, the customer on whose behalf the transaction is cleared is the customer for AML/CTF purposes.

18.43 A customer may choose to use one or more executing brokers because:

- the customer may prefer, for reasons of functionality or cost, the executing broker's front-end electronic order routing;
- certain brokers develop a reputation for being able to execute transactions very efficiently in certain contracts, while the clearing broker provides superior post-trade clearing and settlement services;
- the customer may feel more comfortable with the credit risk of the clearing broker;
- the executing broker may provide access to certain value-added services linked to the execution of the customer's transactions; or
- the customer does not wish to disclose its trading strategy to other market participants; or for other reasons relevant to the customer's business.

18.44 In all give-up arrangements the customer, the executing broker, and the clearing broker are participants. Although this type of tri-partite arrangement is most common, give-up arrangements can extend to cover many types of relationships, and may extend through a number of parties with differing roles and responsibilities including advising, managing, clearing or executing, for or on behalf of the underlying customer, before the trade reaches the ultimate clearing broker.

18.45 A common additional participant in a give-up arrangement is the customer's investment adviser or manager, who in the give-up agreement is usually referred to as a trader, to whom the customer has granted discretionary trading authority, including the authority to enter into give-up arrangements on the customer's behalf.

18.46 Typically, an adviser or manager acting for a client may only wish to disclosure a reference code, rather than their client's name, to the executing broker, particularly where the adviser or manager has multiple underlying accounts over which they exercise discretionary authority; hence, the clearing broker is likely to be the only party that knows the underlying customer's identity. Where a give-up agreement includes such an arrangement, firms should ensure that their risk-based approach addresses the risks posed, which may include the risk associated with the investment manager as appropriate, the type of fund and possibly the underlying investors. Hence, where a firm is acting as executing broker and there is a adviser or manager acting for an underlying customer, the customer due diligence performed, and whether there is an obligation to identify the underlying customer, will depend upon the regulatory status and location of the adviser or manager. For further guidance, see Part I, section 5.3. Where simplified due diligence cannot be applied to the adviser or manager and there is an obligation to verify the identity of the adviser or manager and their underlying customers, the firm should take a risk-based approach (see Part I, Chapter 5, section 5.3), which may include consideration of whether it is appropriate, subject to satisfying the ML Regulations, to take into account any verification evidence obtained by, a clearing broker in the UK, EU or an equivalent jurisdiction.

18.47 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 itself a regulated firm from an equivalent jurisdiction, the executing broker may wish to rely upon the clearing broker if they are a 'third party' as defined in the ML Regulations (see Part I, Chapter 5, paragraph 5.6.4ff) or otherwise take account of the fact, in its risk-based approach, that there is another regulated firm from an equivalent jurisdiction involved in the transaction with the customer, acting as clearing agent or providing other services in relation to the transaction.

18.48 Given the information asymmetries likely to exist between an executing broker and clearing broker, when a firm is acting as clearing broker, it would generally not be appropriate, from a risk-based perspective, to rely on an executing broker, even if this would be permitted under the ML Regulations. Clearing firms should undertake the CDD measures as set out in Part I, Chapter 5.

(c) Executing brokers and clearing brokers: securities markets

18.49 There are fundamentally two types of arrangements that can exist in relation to the outsourcing of clearing and settlement processes in the securities markets. These are generally known as "Model A" and "Model B" clearing relationships. The specific characteristics of these relationships are outlined below.

"Model A" Clearing

18.50 Model A clearing usually involves the outsourcing of the settlement processing of transactions executed by a firm to a service provider. All transactions are executed and settled in the name of the executing firm, who retains full responsibility, including financial liability, for the transaction in relation to both the underlying customer and the market counterparty. The underlying customer remains solely a customer of the executing firm, which retains AML/CTF responsibility, and does not enter into a relationship with the settlement services provider.

18.51 The settlement services provider maintains a relationship solely with the executing firm, and acts as an agent on behalf of the executing firm. As such, the settlement services provider has no obligation to undertake the identification and verification requirements set out in Part I, Chapter 5, other than in relation to its customer, the firm.

"Model B" Clearing

18.52 In the securities markets, the executing broker/clearing firm arrangements are commonly referred to as "Model B" clearing arrangements.

18.53 The executing broker will usually open an account (or sub-accounts) with the clearing firm, in the name of his underlying customer, and will fulfil all verification and due diligence requirements on the underlying customer. A tri-partite relationship between the underlying customer, the executing broker and the clearing firm (the 'tripartite relationship') is created, by virtue of the fact that the executing broker has entered into a Model B clearing relationship with the clearing firm on his own behalf, and, acting as the agent of the customer.

18.54 Usually, the customer does not establish a relationship direct with the clearing firm, but rather will enter into the tri-partite relationship via the executing broker, which has a Model B clearing relationship with the clearing firm. There is little or no contact between the underlying customer and the clearing firm. The customer is generally unable to terminate his relationship with the executing broker whilst retaining a relationship with the clearing firm in isolation.

18.55 Should the executing broker terminate its relationship with the clearing firm, the underlying customer will move with the executing broker. If the clearing firm has provided custody services as part of the services being supplied to the executing broker, consent to transfer the assets is required, with any residual transfer of assets for non-responding customers usually being subject to a rule waiver from the FSA upon fulfilment of certain conditions.

18.56 Whilst, under a Model B relationship, the transaction is 'given up' to the clearing firm for settlement with the market, if the underlying customer fails to deliver funds or assets to fulfil settlement, the clearing broker may look to the executing broker to offset any outstanding liabilities through a secondary deposit or other funds held by the clearing firm on behalf of the executing broker. In turn, the executing broker would have to pursue the underlying customer for fulfilment of settlement/debt recovery.

18.57 Because the relationship with the underlying customer is always focused through the executing broker, the executing broker remains an integral part of the relationship and transaction process at all times. This is by virtue of the tri-partite relationship, rather than separate relationships between the executing broker and the underlying customer, and the underlying customer and the clearing firm. Therefore, the CDD measures set out in Part I, Chapter 5, are generally undertaken by the executing broker while the clearing firm may, if it considers it appropriate to do so under its risk-based approach, rely upon the executing broker provide that broker is a 'third party' as defined in the ML Regulations (see Part I, Chapter 5, paragraph 5.6.4ff).

(d) Non-clearing members and general clearing members: derivatives / securities markets

18.58 A non-clearing member may maintain one or several accounts with the 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.

18.59 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.

18.60 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.

(e) Other multi-partite agreements

18.61 Multi-partite agreements are common in a number of markets, for example, as part of prime brokerage services. Further guidance on the 'give-up' arrangements for exchange traded derivatives - parts of which may be relevant in other markets - is set out above, while firms involved in multipartite agreements in respect of unregulated funds should refer to sector 20: *Unregulated Funds.*

Customer due diligence

18.62 Product risk alone should not 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.

18.63 To avoid unnecessary duplication where an executing broker and a clearing broker are involved in the same transaction on behalf of the same customer, which is subject to a give-up arrangement, the executing broker in the exchanged-traded derivatives markets or a clearing broker under a Model B clearing arrangement may, where as part of its risk-based approach it feels it is appropriate to do so:

- place reliance on the other regulated firm involved in the transaction with the customer provided they are regulated in the UK, another EU Member State or an equivalent jurisdiction and the requirements for third party reliance in the ML Regulations are satisfied. Guidance on reliance on third parties and on the factors to consider, as part of a firm's risk-based approach, when seeking to rely on another firm to apply the CDD measures (but not monitoring) is given in Part I, Chapter 5, paragraphs 5.6.4ff.; **or**
- otherwise take account of the fact, in its risk-based approach, that there is another regulated firm from the UK/EU or an equivalent jurisdiction involved in the transaction with the customer, acting as clearing agent or providing other services in relation to the transaction, without placing reliance on the firm.

Monitoring

18.64 The money laundering or terrorist financing risks for firms operating within the wholesale markets sector can be mitigated by the implementation of monitoring procedures. Guidance on general monitoring requirements is set out in Part I, section 5.7.

18.65 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 a customer's trading activities and it may be difficult to assess the commercial rationale of certain transactions. 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.

18.66 The nature and extent of any monitoring activity will therefore need to be determined by a firm based on an assessment of their 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
- Payment processes (including payments to third parties, if permitted)

18.67 Firms should ensure that any relevant factors taken into account in determining their monitoring activities are adequately documented and subject to periodic review.

18.68 Firms relying on third parties under the ML Regulations to apply CDD measures **cannot** rely on the third party in respect of monitoring.

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 FSA 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.

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: Servicing unregulated 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 for firms servicing unregulated funds in a number of specific situations: executing transactions, clearing and settling transactions and offering other prime brokerage services. 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 may want to take into account when considering applying a risk-based approach.

A firm's business activities with unregulated funds may also fall within the scope of other sectoral guidance, for example, sector 18: *Wholesale Markets* and sector 9: *Discretionary and advisory investment management.* As such, this sectoral guidance should be read together with other applicable parts of the guidance.

Overview of the sector

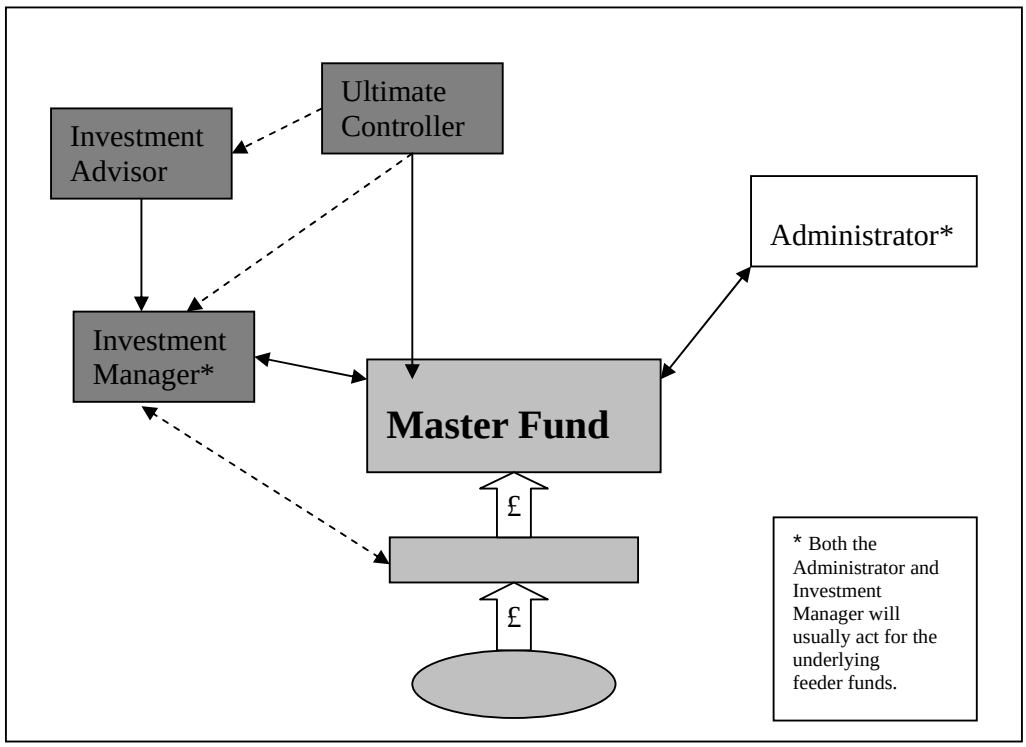
20.1 An unregulated fund is a vehicle established to hold and manage investments and assets, which is not subject to regulatory oversight. The fund usually has a stated purpose and/or set of investment objectives. Unregulated funds will normally be a separate legal entity, formed as limited companies, limited partnerships and trusts (or the equivalent in civil law jurisdictions).

20.2 Unregulated funds are stand-alone entities in order that the assets and liabilities may be restricted to the fund itself. Sub-funds typically take the form of different classes of shares, fund allocations to separately incorporated trading vehicles or legally ring-fenced portfolios.

20.3 Unregulated funds may also operate as a "master/feeder" arrangement, whereby investors, perhaps 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 act for a fund acting in its own right whilst also at the same time being a feeder fund.

20.4 Dependent upon structure, an unregulated 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 following diagram sets out the relationships that exist and are involved with the operation and management of an unregulated fund:



- **Ultimate Controllers**
  The ultimate controller is someone who controls the funds/assets in the fund. The ultimate controller may be a different person/entity in different fund set-ups. Sometimes it can be the investment manager, the adviser, or directors of other related parties, who may delegate this responsibility. The place to look for those who are the ultimate controllers is usually the fund's offering memorandum.

- **Investment Manager**
  Unregulated funds are managed by an investment manager, which is a separate entity to the fund, and which is given authority to 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 on behalf of the unregulated fund. The investment manager plays a pivotal role within an unregulated fund structure, as it establishes and maintains the relationships with the Prime, Clearing and Executing brokers and will be the direct contact with a firm on behalf of the fund. A firm may also act as investment manager to a fund. Investment managers may or may not be regulated, depending upon the jurisdiction they are registered in or operate from, and therefore be subject to varying degrees of regulatory oversight. 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

    a) the selection of investors,
    b) the investment strategy of the fund, and
    c) the placement of orders.

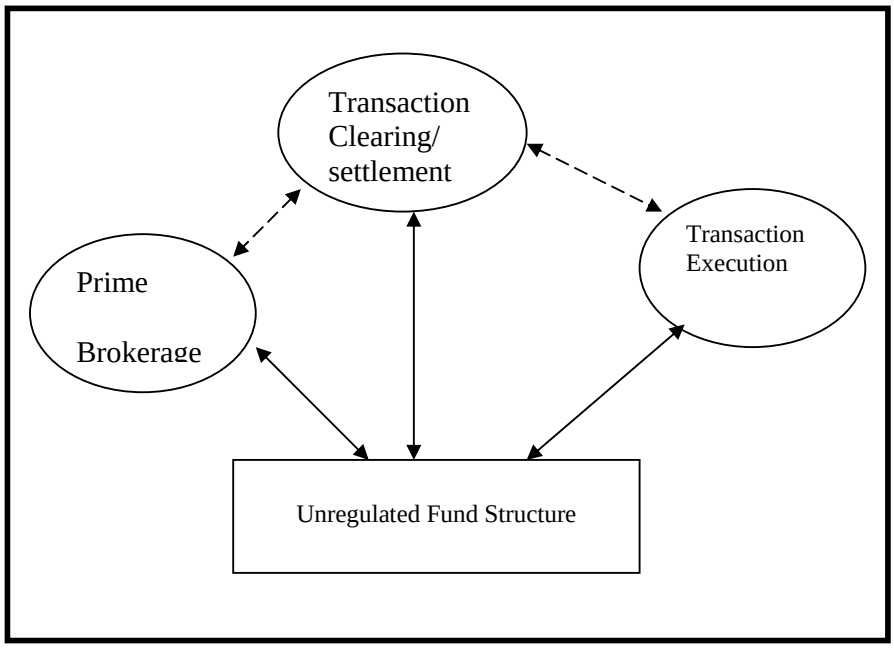
A fund may have more than one investment manager, known as sub-managers. Sub-managers are responsible for managing/investing part of the fund, and, depending on the structure of the fund, there may be more than one sub-manager.

- **Investment Adviser**
  Some unregulated 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.

- **Administrator**
  Administrative services such as the day to day operation of the fund and routine tasks associated with managing investments on behalf of investors will be undertaken by a separate entity know as the fund's Administrator. Although providing administrative services is not regulated activity in UK (although it may be in other jurisdictions), a firm itself or a sister company of a regulated entity may provide administrative services to a fund.

- **Other Relationships**
  In addition to the above-mentioned entities involved in the operation and management of the fund, other parties may 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.

20.6 The following diagram sets out the likely relationships a firm may have with an unregulated fund.



- **Transaction Execution**
  Transactions or trading are undertaken for an unregulated fund by a firm commonly known as an executing broker. An unregulated fund may elect to execute transactions through one or more firms. The executing broker takes instructions from the unregulated fund or its appointed agent (usually the investment manager), but passes the transactions/trades to a clearing broker for clearing and settlement.

- In derivative transactions the executing broker gives up the transaction to a clearing broker for settlement.

- 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.

- **Clearing/Settlement**
  An unregulated 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 unregulated fund, and as such will handle the movement of funds or assets from the unregulated fund in settlement of the unregulated fund's transactions and liabilities.

- **Prime Brokerage Services**
  Prime brokerage is the provision of brokerage products and services to an unregulated fund. Prime brokerage is a portal to a suite of products and services offered by a prime brokerage such as custody, reporting, securities lending, cash lending, leverage and pricing. Some prime brokers provide capital introduction, start-up services, credit intermediation, risk management, straight-through processing, futures and options clearing, research, initial public offerings and contacts for difference and swaps. Most unregulated funds will only appoint one firm as its prime broker to undertake all or some of the above activities for it. Some unregulated funds may, however, not have a prime broker.

- **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 unregulated fund by the investment manager.

What are the money laundering risks associated with unregulated funds?

20.7 Unregulated 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 unregulated funds will, in most cases, not be known to the firm providing services to the unregulated fund;
- The unregulated status of the fund implies that it may be more difficult to ensure that the AML requirements applied to investors are of the appropriate standard;
- An unregulated 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 an unregulated 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 unregulated fund trading activity and the complexity of underlying trading strategies; and
- The fund may accept nominee investments.

How to assess the elements of risk

20.8 The level of risk actually posed by the unregulated 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.

20.9 The status and reputation of other service providers, such as executing, clearing or prime brokers and the administrator, may also be a factor in determining the risks associated with an unregulated fund.

20.10 Where a firm agrees to undertake third party payments on behalf of an unregulated fund, the risk 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 review of these types of payments and receipts, as well as ensuring appropriate levels of sign-off with the firm.

Who is a firm's customer for AML purposes?

20.11 Where the firm's customer qualifies for the treatment of simplified due diligence (see Part I, section 5.4), no customer due diligence is required. This would be true even where the firm is aware that its customer is acting on behalf of an underlying customer who would not itself qualify for simplified due diligence; no question of reliance under Regulation 17 will arise.

20.12 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 the unregulated fund. 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.

- Where the firm is acting as the investment manager or investment adviser[14] for a fund, for AML purposes the fund is the customer of the firm.

- Where the firm is acting as the administrator to the fund, for AML purposes the fund is the customer of the firm.

- Where the firm is acting as an executing broker, the customer for AML purposes may be the unregulated 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.

- 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, unless otherwise agreed by the parties.

[14] References to Investment Manager in this section also refer to Investment Adviser

- Where the agent is unregulated, or regulated within a non-equivalent jurisdiction, both the agent and the underlying fund will be considered to be customers for AML purposes.

- Where the firm is acting as clearing broker and/or settlement agent the customers for AML purposes will be the fund.

- Where the firm is providing prime broker services, the customer for AML purposes will be the fund.

20.13 Within a firm, other departments such as risk, operations, legal or credit may identify other parties as being relevant to the relationship and undertake their own due diligence processes on those parties. A firm may, as part of its AML process, take this into account. For AML purposes, however, verification of identity and information-gathering on these parties may not be necessary as these parties may not be relevant to AML customer due diligence requirements.

Customer due diligence

20.14 Due to the characteristics of unregulated 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.

20.15 On occasion, practical aspects of unregulated 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.

20.16 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, information on the Feeder Fund's offering memoranda/prospectuses and, in some instances its investors, may also be useful.

- Who places orders and transaction 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.

- 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.

20.17 The unregulated 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.

20.18 Where the unregulated fund has a number of layers of entities in its ownership/control structure, 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.

20.19 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.

20.20 A firm should also undertake due diligence on the entities involved with the fund, namely:

Investment manager

20.21 The identity of the investment manager that has direct contact with the firm, or which instructs the firm on behalf of the unregulated 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) although, as discussed above, under its risk-based assessment a firm may consider it appropriate to identify other parties involved.

Relevant investors

20.22 Shares or units in unregulated funds may be open to general subscription, or to purchase by any qualifying investors. Alternatively, unregulated funds may be established for the exclusive use of a closed group of 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.

20.23 'Relevant investors' i.e., investors who have a 25% or more interest in the fund, however, are also beneficial owners (see Part I, Chapter 5, paragraph 5.3.8ff). Whether a firm has to identify and take risk-based and adequate measure to verify the identity of relevant investors, depends on a number of factors:

- Where the investment manager is the firm's customer and 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) although, as discussed above, under its risk-based assessment a firm may consider it appropriate to identify other parties involved;

- Where the fund, or an unregulated fund manager, 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 5.6.19ff).

- In other cases, if the risk is assessed as lower, a firm may wish to satisfy itself as to the beneficial owners' identity based on information supplied by the customer (see Part I, Chapter 5, paragraphs 5.3.10 and 5.3.11).

- In all other cases - or where, following its assessment of the money laundering risk presented by the unregulated fund, a firm considers it appropriate -a firm should 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.

- Subject to the firm's risk-based approach, a firm whose customer for AML purposes is the unregulated fund or an investment manager to whom simplified due diligence cannot be applied, 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
    - There are no Relevant Investors.

20.24 Where a firm accepts such a representation, this should be documented, retained, and subject to periodic review.

20.25 Although it will often be the administrators to the fund, it is important to establish who in the fund structure is responsible for this process. If the party responsible for verifying the identity of the Relevant Investors is regulated in an equivalent 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.

20.26 However, where the responsible party is not regulated in an equivalent 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.

Start-up funds

20.27 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

20.28 As a minimum, feeder funds themselves should be identified in accordance with the guidance in Part I, Chapter 5.

20.29 Where there are feeder funds, the assets/money held by the master fund will be owned by them. The feeder funds will be investors in the unregulated fund, and 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

20.30 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.

Ultimate Controllers

20.31 Where, because of the risk profile of the unregulated 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 unregulated 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.

20.32 Ultimate control may be exercised through a chain of entities between the fund and the ultimate controller. This relationship should be established and documented. However, it is not necessary to obtain full identity information or verify the identity of each intermediate entity, or their connected persons that exists between the unregulated fund and its ultimate controller(s).

Feeder Funds

20.33 Where, because of the risk profile of the unregulated 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

20.34 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 from an equivalent 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 equivalent jurisdiction acting as clearing agent or providing other services in relation to the transaction.

20.35 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

20.36 The money laundering risks to firms offering services to unregulated funds can be mitigated by the implementation of monitoring procedures; guidance on the general monitoring

requirements are set out in Part I, section 5.7. However, there are specific characteristics of unregulated funds which will be relevant, in particular the use of multiple brokers.

20.37 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.

20.38 Monitoring unregulated 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.

20.39 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 unregulated funds who are customers (e.g., geographic location)
- Number of customers and volume of transactions
- Types of products traded and complexity of those products
- Payment procedures

20.40 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.

20.41 Firms relying on third parties under the ML Regulations to apply CDD measures **cannot** rely on the third party in respect of monitoring.

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 the detail of all their 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. As the assignment is not usually disclosed the client undertakes the collection service 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. The non-disclosure element has led to the frequent use of the colloquial title of Confidential Invoice Discounting being used to describe this 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 is provided against a 'basket' of assets – accounts receivables, inventory, plant machinery, property, etc.

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. 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 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, cash) 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 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.

21.16 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.

21.17 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 SOCA.

21.18 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 SOCA.

Assessment of risk

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.

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.

21.29 Where invoice finance companies are involved in arrangements with Affiliated Factoring Companies, the customer is as defined in sector 16: *Correspondent Banking*. In such cases, the guidance in sector 16 should be read in addition to the guidance in this part of the Guidance.

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 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 underlying customers 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 5.5.1-5.5.8 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.

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.

Specialist guidance

A: Wire transfers

Note: This sectoral guidance will only be relevant to a limited number of firms in the financial sector (see Part I, paragraphs 5.2.10ff)

Background

A.1 FATF issued Special Recommendation VII in October 2001, with the objective of enhancing the transparency of electronic payment transfers ("wire transfers") of all types, domestic and cross border, thereby making it easier for law enforcement to track funds transferred electronically by terrorists and criminals. A revised Interpretative Note to this Special Recommendation was issued by the FATF on 10 June 2005, and is available at http://www.fatf-gafi.org/dataoecd/34/56/35002635.pdf

A.2 Special Recommendation VII is addressed to FATF member countries, and has been implemented in member states of the European Union, including the UK, through a Regulation issued by the European Parliament and the Council of the European Union.

A.3 This Regulation was proposed by the European Commission on 26 July 2005 to implement Special Recommendation VII within the EU with effect from 1 January 2007. In its final form the Regulation was approved by the European Parliament on 6 July 2006 and by the ECOFIN Council on 7 November 2006. It was published in the Official Journal of the European Union (OJ L 345) on 8 December 2006 (EC Regulation 1781/2006).

A.4 Whilst the Regulation has been in force since 1 January 2007, sanctions for non-compliance will not be enforced until 15 December 2007, coincident with the deadline for implementation of the Third EU Money Laundering Directive.

A.5 The Regulation can be found at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_345/l_34520061208en00010009.pdf

A.6 The Regulation requires the ordering financial institution to ensure that all wire transfers carry specified information about the originator (Payer) who gives the instruction for the payment to be made. The core requirement is that this information consists of name, address and account number; however, there are a number of permitted variations and concessions, see below under **Information Requirements** (paragraphs A.15ff**).**

A.7 As the text of this Regulation has EEA relevance, the three non-EU Member States of the EEA, i.e., Iceland, Liechtenstein and Norway, are expected to enact equivalent legislation. As and when this happens, references in this guidance to *intra-EU* can be understood to include these states. However, for the time being the reduced information requirement available within the EU will not apply to payments to and from those countries.

Scope of the Regulation

A.8 The Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made "by electronic means", other than those specifically exempted wholly or partially by the Regulation. For UK-based Payment Service Providers (PSPs) it therefore includes, but is not necessarily limited to, international payment transfers made via SWIFT,

including various Euro payment systems, and domestic transfers via CHAPS and BACS. The Regulation specifically exempts the following payment types:

- transfers where both Payer and Payee are PSPs acting on their own behalf - this will apply to MT 200* series payments via SWIFT. This exemption will include MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks (*cover payments using MT 202s are technically in scope but until the message format is changed the MT 202 will not itself carry payer information, although its associated MT103 must do so.);

- transfers by credit or debit card or similar payment instrument, providing that the Payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the Payer (see paragraph A.18);

- transfers whereby the Payer withdraws cash from his/her own account. This is designed to exempt ATM withdrawals outside the EU which would otherwise attract the full information requirement;

- transfers to public authorities for taxes, fines or other levies;

- direct debits, subject to their carrying a unique identifier for tracing purposes;

- truncated cheques (cheques are otherwise paper to which the Regulation does not apply);

- Article 3 (4) provides a limited exemption for small pre-paid transfers carried out by means of a mobile phone or any other digital or IT device;

- e-money transfers, as defined in Article 11(5)(d) of the Third EU Money Laundering Directive, where they do not exceed €1000. i.e., those transfers transacted using non-reloadable electronic money products on which the maximum load does not exceed € 150, or using reloadable e-money products which are subject to a maximum load of €2500 in a calendar year and maximum redemption of under €1000 in the same calendar year. (see also Sector 3: *Electronic money*);

- post-paid funds transfers carried out by mobile phone, or any other digital or IT device, subject to various conditions, including their traceability and that they relate to the provision of goods and services.

A.9 The following payment types are also exempt under the Regulation (under derogations which are not used in the UK):

- Article 3 (6), which exempts small payments for goods and services, relates to giro payment systems in a few other member states;

- funds transfers of €150 or less for charitable, religious, cultural, educational, social, scientific or fraternal purposes to a prescribed group of non-profit organisations which run annual / disaster relief appeals and which are subject to reporting and external audit requirements or supervision by a public authority and whose names and supporting details have been specifically communicated by the Member State to the Commission. This applies only to transfers within the territory of the Member State. The exemption is designed to ensure that small charitable donations to certain bona fide bodies are not frustrated, but has limited practical relevance in the UK, where typical mechanisms for making payments to charities,

e.g., by credit transfer or by card payment within the EU, will either not be subject to the Regulation, or where they are, will be compliant with it in any case;

A.10 The UK credit clearing system is out of scope of the Regulation as it is paper-based and hence transfers are not carried out "by electronic means". Cash and cheque deposits over the counter via bank giro credits are not therefore affected by the Regulation.

Note: The Regulation defines "Payee" as a natural or legal person who is the intended final recipient of transferred funds. Recognizing that a perverse and wholly unworkable interpretation could be put on those words, where a named Payee might have been a conduit for an undisclosed 'final recipient' to serve a criminal objective, this Guidance takes the position that 'final recipient' can only practically be understood as referring to the party named in the transfer as the beneficiary of the payment.

Pre-conditions for making payments

A.11 Payment Service Providers (PSPs) of Payers must ensure that the Payer information conveyed in the payment relating to account holding customers is accurate and has been verified. The verification requirement is deemed to be met for account holding customers of the PSP whose identity has been verified, and where the information obtained by this verification has been stored in accordance with anti money laundering requirements, ie in the UK in accordance with the Money Laundering Regulations which will give effect to the Third EU Money Laundering Directive. This position applies even though the address shown on the payment transfer may not have been specifically verified. No further verification of such account holders is required, although PSPs may wish to exercise discretion to do so in individual cases; e.g., firms will be mindful of Part I, paragraphs 5.3.14 – 5.3.18, concerning customers with existing relationships. (See A.14ff where the named Payer is not the holder of the account to be debited.)

A.12 Before undertaking one-off payments in excess of €1000 on the instructions of non-account holding customers, the PSP of the Payer should verify the identity and address (or evidence of a permitted alternative to address, such as date and place of birth if quoting that information on the transfer instead of address).

A.13 For non-account based transfers of €1000 and under, PSPs are not required by the Regulation to verify the Payer's identity except when several transactions are carried out which appear to be linked (see Article 5.4) and together exceed €1000. NB, even in cases where the Regulation does not require verification, the customer information has to be obtained and it may be advisable for the PSP to verify the identity of the Payer in all cases.

A.14 Evidence of verification must be retained with the customer information in accordance with **Record Keeping Requirements** (see A.20-A.21).

Information Requirements

A.15 Complete payer information:

Except as permitted below, complete Payer information must accompany all wire transfers. Effectively, the complete Payer information requirement applies where the destination PSP is located in a jurisdiction outside the European Union. Complete Payer information consists of: name, address and account number.

- Address ONLY may be substituted with the Payer's date and place of birth, or national identity number or customer identification number. This Guidance recommends that these options are only deployed selectively within a firm's processes to address particular needs. It follows that in the event a Payee PSP demands the Payer's address, where one of the

alternatives had initially been provided, the response to the enquiry should point that out. Only with the Payer's consent or under judicial compulsion should the address be additionally provided.

- Where the payment is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier which permits the payment to be traced back to the Payer.

- The extent of the information supplied in each field will be subject to the conventions of the messaging system in question and is not prescribed in detail in the Regulation.

- The account number could be, but is not required to be, expressed as the IBAN (International Bank Account Number).

- The Regulation applies even where the Payer and Payee hold accounts with the same PSP.

- Where a bank is itself the Payer, as will sometimes be the case even for SWIFT MT 102 and 103 messages, this Guidance considers that supplying the Bank Identifier Code (BIC) constitutes complete Payer information for the purposes of the Regulation, although it is also preferable for the account number to be included where available. The same applies to Business Entity Identifiers (BEIs), although in that case the account number should always be included. As the use of BICs and BEIs is not specified in FATF Special Recommendation VII or the Regulation, there may be requests from Payee PSPs for address information.

- Generally, firms will populate the information fields from their customer database. In cases where electronic banking customers input their details directly the Payer's PSP is not required, at the time that the account is debited, to validate the Payer's name and/or address against the name and address of the accountholder whose account number is stated on the payment transfer.

- Where the named Payer is not the accountholder the Payer's PSP may either substitute the name and address (or permitted alternatives) of the account holder being debited (subject to any appropriate customer agreement), or execute the payment instruction with the alternative Payer name and address information provided with the consent of the accountholder. In the latter case, provided the Payer PSP retains all relevant data for 5 years, the Payer PSP is required to verify only the information about the accountholder being debited (in accordance with Article 5.3a. of the Regulation). PSPs should exercise a degree of control to avoid abuse of the discretion by customers.

  It is important to note that this flexibility should not undermine the transparency of Payer information sought by FATF Special Recommendation VII and the Regulation. It is designed to meet the practical needs of corporate and other business (e.g., solicitor) accountholders with direct access who, for internal accounting reasons, may have legitimate reasons for quoting alternative Payer details with their account number.

- Where payment instructions are received manually, for example, over the counter, the Payer name and address (or permitted alternative) should correspond to the account holder. Any request to override customer information on a similar basis to that set out above for electronic banking customers should be contained within a rigorous referral and approval mechanism to ensure that only in cases where the PSP is entirely satisfied that the reason is legitimate should the instruction be exceptionally dealt with on that basis. Any suspicion of improper motive by a customer should be reported to the firm's Nominated Officer.

A.16 Reduced Payer Information:

Where the PSPs of both Payer and Payee are located within the European Union, wire transfers need be accompanied only by the Payer's account number or by a unique identifier which permits the transaction to be traced back to the Payer.

- However, if requested by the Payee's PSP, complete information must be provided by the Payer's PSP within three working days, starting the day after the request is received by the Payer's PSP. ("Working days" is as defined in the Member State of the Payer's PSP).

- Article 17 of the Regulation provides for the circumstances in which transfers of funds between EU Member States and territories outside the EU with whom they share a monetary union and payment and settlement systems may be treated as transfers within the Member State, so that the reduced information requirement can apply to payments passing between that Member State and its associated territory (but not between any other Member State and that territory). In the case of the UK such arrangements will include the Channel Islands and the Isle of Man.

A.17 Batch File Transfers:

A hybrid complete/reduced requirement applies to batch file transfers from a single Payer to multiple Payees outside the EU in that the individual transfers within the batch need carry only the Payer's account number or a unique identifier, provided that the batch file itself contains complete Payer information.

A.18 Payments via Intermediaries:

Intermediary PSPs (IPSPs) must, subject to the following guidance on technical limitations, ensure that all information received on the Payer which accompanies a wire transfer is retained with the transfer.

It is preferable for an IPSP to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an IPSP within the EU is technically unable to on-transmit Payer information originating outside the EU, it may nevertheless use a system with technical limitations provided that:

- if it is aware that the Payer information is missing or incomplete it must concurrently advise the Payee's PSP of the fact by an agreed form of communication, whether within a payment or messaging system or otherwise.

- it retains records of any information received for five years, whether or not the information is complete. If requested to do so by the Payee's PSP, the IPSP must provide the Payer information within three working days of receiving the request.

A.19 Card transactions

As indicated in paragraph A.8, card transactions for *goods and services* are out of scope of the Regulation provided that a unique identifier, allowing the transaction to be traced back to the payer, accompanies the movement of the funds. The 16 digit Card PAN number serves this function.

Similarly, the Card PAN number meets the information requirement for all Card transactions for any purpose where the derogation for transfers within the European Union applies, as explained in and subject to the conditions set out in paragraph A.15.

Complete payer information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a payee whose PSP is located outside the EU. These are "push" payments, and as such capable of carrying the information when required under the Regulation.

Otherwise, Card transactions are "pull" payments, i.e., the transfer of funds required to give effect to the transaction is initiated by the merchant recipient rather than the Card Issuer and under current systems it is not possible for any information in addition to the PAN number to flow with the transfer in those cases where the transaction is arguably not for 'goods and services' but is settled to a PSP outside the EU. Examples include Card transactions used to make donations to charity, place bets, or purchase e-money products such as prepaid cards. As a matter of expediency these transactions must therefore be treated as 'goods and services'. FSA and HM Treasury have supported that interpretation for the time being, subject to further review at an unsecified future date on the basis that the transactions are traceable by the PAN number.

A.20 Minimum standards

The above information requirements are minimum standards. It is open to PSPs to elect to supply complete Payer information with transfers which are eligible for a reduced information requirement and thereby limit the likely incidence of inbound requests for complete information. (In practice a number of large UK and European banks have indicated that they will be providing complete payer information for all transfers where systems permit). To ensure that the data protection position is beyond any doubt, it would be advisable to ensure that terms and conditions of business include reference to the information being provided.

Record Keeping Requirements

A.21 The Payee's PSP and any intermediary PSP must retain records of any information received on a Payer for five years, in accordance with the Regulation.

A.22 The Payer's PSP must retain records of transactions and supporting evidence of the Payer's identity in accordance with Part I, Chapter 8.

Checking Incoming Payments

A.23 Payee PSPs should have effective procedures for checking that incoming wire transfers are compliant with the relevant information requirement. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer. The Regulation specifies that PSPs should have procedures to detect whether relevant information is missing. (It is our understanding that this requirement is satisfied by the validation rules of whichever messaging or payment system is being utilised). Additionally, the Regulation requires PSPs to take remedial action when they become aware that an incoming payment is not compliant. Hence, in practical terms it is expected that this requirement will be met by a combination of the following:

(i) SWIFT payments on which mandatory Payer information fields are not completed will fail anyway and the payment will not be received by the Payee PSP. Current SWIFT validation prevents payments being received where the mandatory information is not present at all. However, it is accepted that where the Payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system. SWIFT is currently considering how its validation standards might be improved to respond more effectively to the requirements of FATF Special Recommendation VII. Similar considerations apply to non-SWIFT messaging systems which also validate that a field is populated in accordance with the standards applicable to that system, e.g., BACS.

(ii) PSPs should therefore subject incoming payment traffic to an appropriate level of post event random sampling to detect non-compliant payments. This sampling should be risk based, e.g.,:

- the sampling could normally be restricted to payments emanating from PSPs outside the EU where the complete information requirement applies;

- the sampling could be weighted towards non FATF member jurisdictions, particularly those deemed high risk under a PSP's own country risk assessment, or by reference to external sources such as Transparency International, or FATF or IMF country reviews);

- focused more heavily on transfers from those Payer PSPs who are identified by such sampling as having previously failed to comply with the relevant information requirement;

- Other specific measures might be considered, e.g., checking, at the point of payment delivery, that Payer information is compliant and meaningful on all transfers that are collected in cash by Payees on a "Pay on application and identification" basis.

  NB. None of the above requirements obviate the obligation to report suspicious actions (see Part I, Chapter 6).

A.24 If a Payee PSP becomes aware in the course of processing a payment that it contains meaningless or incomplete information, under the terms of Article 9 (1) of the Regulation it should either reject the transfer or ask for complete information on the Payer. In addition, in such cases, the Payee PSP is required to take any necessary action to comply with any applicable law or administrative provisions relating to money laundering and terrorist financing. Dependent on the circumstances such action could include making the payment or holding the funds and advising the Payee PSP's Nominated Officer.

A.25 Where the Payee PSP becomes aware subsequent to processing the payment that it contains meaningless or incomplete information either as a result of random checking or other monitoring mechanisms under the PSP's risk-based approach, it must:

(i) seek the necessary information on the Payer

and/or

(ii) take any necessary action under any applicable law, regulation or administrative provisions relating to money laundering or terrorist financing.

A.26 PSPs will be mindful of the risk of incurring civil claims for breach of contract and possible liability if competing requirements arise under national legislation, including in the UK the Proceeds of Crime Act and other anti money laundering and anti terrorism legislation.

A.27 Where a PSP is identified as having regularly failed to comply with the information requirements, the Payee PSP should take steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that PSP or deciding whether to terminate its relationship with that PSP either completely or in respect of funds transfers.

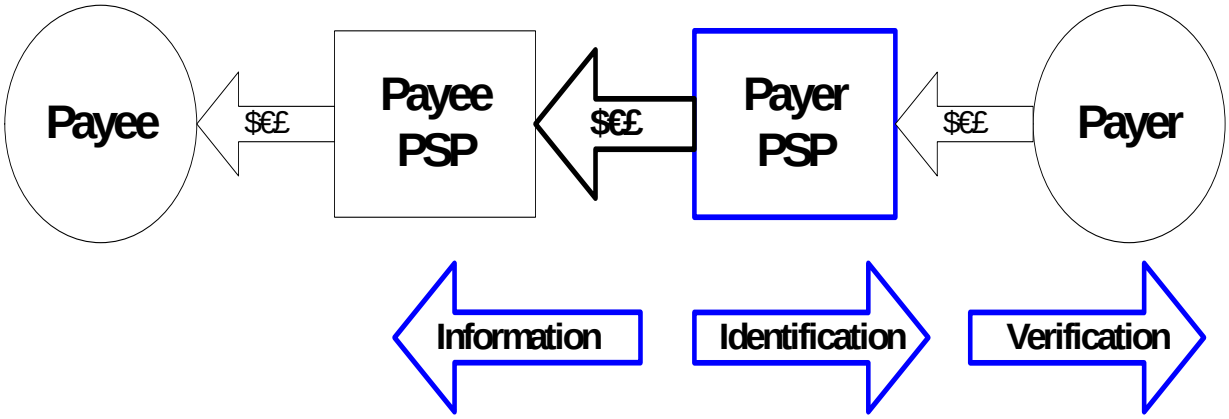
A.28 A Payee PSP should consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion which would be reportable to its Nominated Officer for possible disclosure to the Authorities.

A.29 With regard to transfers from PSPs located in countries that are not members of either the EU or FATF, firms should endeavour to transact only with those PSPs with whom they have a relationship that has been subject to a satisfactory risk-based assessment of their anti money laundering culture and policy and who accept the standards set out in the Interpretative Note to FATF Special Recommendation VII.

A.30 It should be borne in mind when querying incomplete payments that some FATF member countries outside the EU may have framed their own regulations to incorporate a threshold of €/US$ 1000 below which the provision of complete information on outgoing payments is not required. This is permitted by the Interpretative Note to FATF Special Recommendation VII. The USA is a case in point. This does not preclude European PSPs from calling for the complete information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether or how far to press the point.

Appendix I

Scenario 1: Transfer of funds – Obligations on Payer PSP



Information

If to PSP outside the EU:
- Complete information

If batch file from single payer to PSP outside the EU:
- Complete information on batch
- Account number (or unique identifier) on single transaction

If both PSPs within the EU:
- Account number (or unique identifier)

Identification

Complete Information (CIP):
- Name
- Address (or date and place of birth, or customer identificatio number or national identity number)
- Account number (or unique identifier)

Verification

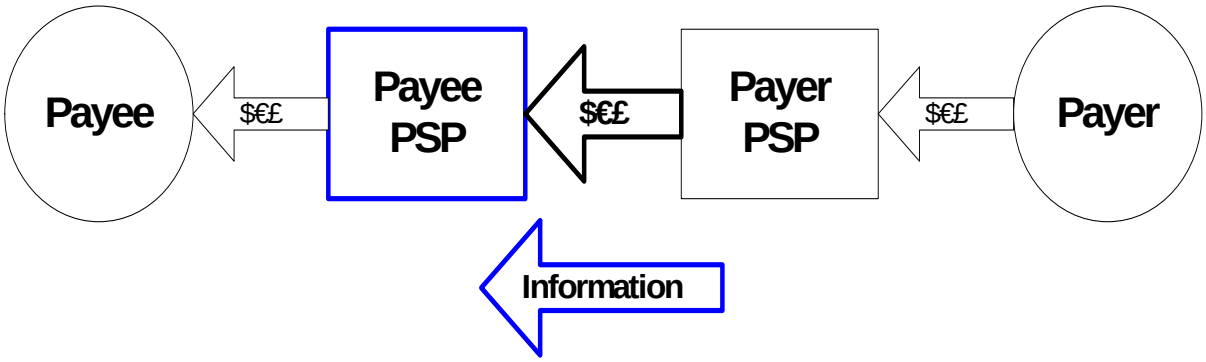
If transaction not from account with PSP:
- If below £650: No mandatory verification of CIP.
- If exceeds £650 or series of linked transactions exceeding £650: Verify CIP.

If transaction from account with the PSP (for any value):
- Verification deemed to have taken place if identity of account holder verified to meet AML requirements.

Records of CIP which accompanies transfer of funds to be kept for 5 years.

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.

Scenario 2: Transfer of funds – Obligations on Payee PSP



Procedures:
- Detect whether appropriate type of information attached and whether fields complete

If fields incomplete or information inappropriate:
- Ask for information or reject transaction
- Decide whether to report to law enforcement

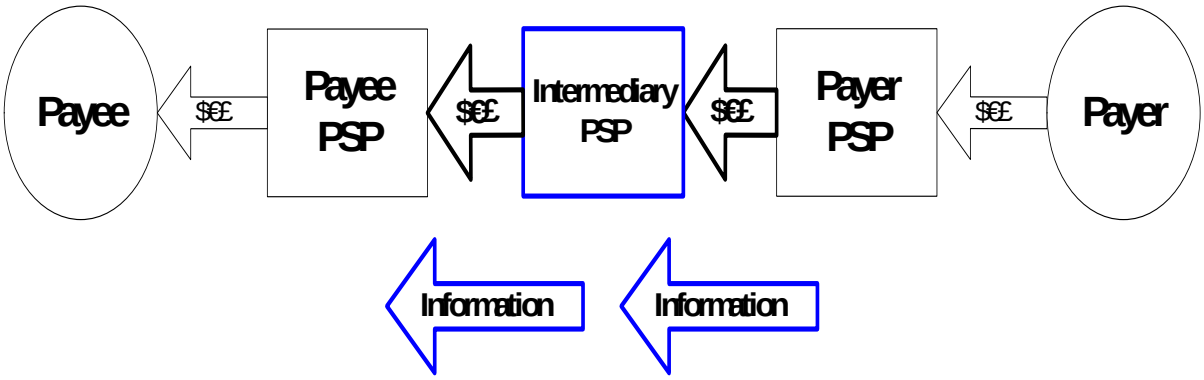
If fields regularly incomplete or information inappropriate:
- Issue warning to PSP of payer
- If no improvement, reject any further transactions or restrict / termniate business relationship
- Report to law enforcement

Note: In practice the procedures required to 'detect' may be met by a combination of system (e.g. SWIFT) validation and risk-based post event random sampling. See Part II, Specialist guidance A: *Wire Tranfers,* A.23 - 30.

Records of any information received to be kept for 5 years

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.

Scenario 3: Transfer of funds – Obligations on Intermediary PSP



Keep information received with the transfer. Where technical limitations prevent this see Part II, Specialist guidance A: *Wire Transfers*, A.18.

Where information is not sent with transfer it must be kept for 5 years

For transactions using e-money the requirements only apply where the transaction value exceeds £650, or the transaction falls outside the annual turnover and redemption limits allowed under the 3MLD.