The Joint Money Laundering Steering Group

Prevention of money laundering/combating terrorist financing

2017 REVISED VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR PART II: SECTORAL GUIDANCE

June 2017 [Amended November 2017]
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

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

[...] indicates no change to June text
1: Retail banking

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

Overview of the sector

1.1 Retail banking is the provision of standard current account, loan and savings products to personal and business customers by banks and building societies. It covers the range of services from the provision of a basic bank account facility to complex money transmission business for a medium sized commercial business. In this guidance, retail banking does not cover credit cards, which are dealt with in sector 2. For many firms, retail banking is a mass consumer business and will generally not involve close relationship management by a named relationship manager.

1.2 This sectoral guidance refers primarily to business undertaken within the UK. Firms operating in markets outside the UK will need to take account of local market practice, while at the same time ensuring that equivalent CDD and record-keeping measures to those set out in the ML Regulations are applied by their branches and subsidiary undertakings operating in these markets.

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

1.3 There is a high risk that the proceeds of crime will pass through retail banking accounts at all stages of the money laundering process. However, many millions of retail banking transactions are conducted each week and the likelihood of a particular transaction involving the proceeds of crime is very low. A firm’s risk-based approach will therefore be designed to ensure that it places an emphasis within its strategy on deterring, detecting and disclosing in the areas of greatest perceived vulnerability.

1.4 There is an increasing risk of fraudulent applications by identity thieves. However, such applications represent a very small percentage of overall applications for retail banking services.

1.5 The provision of services to cash-generating businesses is a particular area of risk associated with retail banking. Some businesses are legitimately cash based, including large parts of the retail sector, and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify, thus providing grounds for looking more closely at whether the account may be being used for money laundering or terrorist financing.

1.6 The feature of lending is generally that the initial monies advanced are paid into another bank or building society account. Consolidation loans may involve payment direct to the borrower’s creditor, and the amount borrowed in some unsecured lending arrangements may be taken in cash. Repayments are usually made from other bank or building society accounts by direct debit; in most cases, repayments in cash are not encouraged.

1.7 Given that a loan results in the borrower receiving funds from the lender, the initial transaction is not very susceptible of the placement stage of money laundering, although it could form part...
of the layering stage. The main money laundering risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination.

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

Other relevant industry and regulatory guidance

1.9 Firms should make use of other existing guidance and leaflets etc. in this area, as follows:

- See “Fighting Financial Crime” pages on www.fca.org.uk
- “International Students – opening a UK bank account” and “Guidance for people wanting to manage a bank account for someone else” – see www.bba.org.uk

1.10 See also paragraphs 1.39 – 1.42 on financial exclusion.

Customer due diligence

General

1.11 The AML/CTF checks carried out at account opening are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals opening accounts or obtaining services from banks. Firms should co-ordinate these processes, in order to provide as strong a gatekeeper control as possible.

1.12 For the majority of personal applicants, sole or joint, the standard identification evidence set out in Part I, Chapter 5 will be applicable, including, in the case of customers not met face to face, consideration of the additional precautions set out in paragraphs 5.3.85 – 5.3.90. See also 1.36 below.

1.13 Documents that are acceptable in different situations are summarised in Part I, paragraphs 5.3.70 – 5.3.75, together with the principles defining when reliance may be placed on a single document or where more than one is required. A current UK passport or photocard driving licence (containing an in-date photograph – see Part I, paragraph 5.3.77) issued in the UK is likely to be used in the majority of cases, other than in the context of financial exclusion, where a bespoke token may be accepted, as set out in Annex 1-I. Non-UK nationals entering the UK should present their national passports or national identity cards, other than in the context of financial exclusion, where bespoke tokens are referred to in Annex 1-I for refugees and asylum seekers.

1.14 Electronic verification may be also used to meet a firm’s customer identification obligations. However, a firm should first consider whether electronic verification is suitable for its customer base, and should then have regard to the guidance in Part I, paragraphs 5.3.40-5.3.45 and 5.3.79–5.3.84. When using electronically-sourced evidence to verify identity, firms should ensure that they have an adequate understanding of the data sources relied on by the external agencies that supply the evidence. Firms should be satisfied that these sources provide enough cumulative evidence to provide reasonable certainty of a person’s identity, and conform with the guidance set out in Part I, Chapter 5. An electronic check that accesses a single database (e.g., Electoral Register check) is normally not enough on its own to verify identity.

The other documents cited in Part I, paragraph 5.3.76 may be used for UK residents where the standard documents are not available, whether singly or in conjunction, according to the principles set out in that paragraph. For non-UK residents, or persons who have recently Commented [A1]: References to BBA need to be updated to UK Finance throughout all three documents.
Commented [A2]: Only if referring to the organisation. Publications issued before 1 July are still available on the BBA website. So this is OK.
Formatted: Indent: Left: 0 cm, Hanging: 1.25 cm, Outline numbered + level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 15 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.66 cm
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 1.23-1.25).

16.16 Where a firm determines that a particular business relationship or transaction presents a low degree of risk of ML/TF, having taken into account the risk assessment the firm has carried out and the risk factors referred to in Regulation 36(3) (see Part I, paragraph 5.4.2), simplified customer due diligence measures may be applied. Simplified due diligence may also be considered in the following situations:

- Where the source of funds may be used as evidence of identity. See Part I, paragraphs 5.3.102 to 5.3.106.
- Where a variation from the standard is required to prevent a person from being financially excluded (see paragraphs 1.39 – 1.42 and Annex 1-I).
- Products which meet the criteria in Regulation 37(3)(b) of the ML Regulations 2017, e.g., a Junior ISA

16.17 However, a firm should take care with customers whose identity is verified under a variation from the standard and who wish to migrate to other products in due course. The verification of identity undertaken for a basic bank account may not be sufficient for a customer migrating to a higher risk product. Firms should have processes defining what additional due diligence, including where appropriate further evidence of identification, is required in such circumstances.

16.18 Where the incentive to provide a false identity is greater, firms should consider deploying suitable fraud prevention tools and techniques to assist in alerting to false and forged identification. Where the case demands, a firm might require proof of identity additional to the standard evidence.

A customer with an existing account at the same firm

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

16.20 If the customer’s identity has been verified to a standard commensurate with the risk associated with the business relationship, a second account would normally be opened without further identification procedures, (provided the characteristics of the new account are not in a higher risk category than the existing account). Thus, a foreign currency account might require further identification procedures and/or additional customer enquiries but for a new savings account, where the applicant’s existing account had been subject to adequate CDD checks, most firms would not require further identification.

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

16.21 Standard identification procedures will usually apply. In some cases, the firm holding the existing account may be willing to confirm the identity of the account holder to the new firm, and to provide evidence of the identification checks carried out. Care will need to be exercised by the receiving firm to be satisfied that the previous verification procedures provide an appropriate level of assurance for the new account, which may have different risk characteristics from the one held with the other firm.
Where different UK regulated firms in the same group share a customer and (before or after any current customer review) transfer a customer between them, either firm can rely on the other firm’s review checks in respect of that customer. Care will need to be exercised by the receiving part of the group to be satisfied that the previous verification procedures provide an appropriate level of assurance for the new account, which may have different risk characteristics from the one held with the other part of the group.

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

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

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

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

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

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

Many applications for advances are made through brokers, who may carry out some of the customer due diligence on behalf of the lender. In view of the generally low money laundering risk associated with mortgage business and related protection policies, and the fraud prevention controls in place within the mortgage market, use of confirmations from intermediaries introducing customers is, in principle, perfectly reasonable, where the introducer is carrying on appropriately regulated business (see Part I, paragraph 5.6.6) including appointed representatives of FCA authorised firms.

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

Business banking in the Retail sector is by nature a volume business, typically offering services for smaller UK businesses, ranging from sole traders and small family concerns to partnerships, professional firms and smaller private companies (e.g. turnover under £1 million 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.

16.28.29 Essentially, as set out in Part I, Chapter 5, identification should initially focus on ascertaining information about the business and its activities and verifying beneficial owners holding or controlling directly or indirectly, 25% or more of the shares or voting rights, and controllers, and where the business is a limited company, obtaining and verifying the information on the basis set out in Regulation 28(3) in respect of the company.

16.29.30 Uncertainties may often arise with a business that is starting up and has not yet acquired any premises (e.g., X & Y trading as ABC Ltd, working from the director/principal’s home). A search of Companies House may not always produce relevant information if the company is newly formed.

16.30.31 In the case of newly-formed businesses, obtaining appropriate customer information is sometimes not easy. The lack of information relating to the business can be mitigated in part by making sufficient additional enquiries to understand fully the customer’s expectations (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.

16.31.32 Firms may encounter difficulties with validating the business entity, particularly where directorships may not have been registered or updated. It is recommended that where this arises (and firms still feel able to open an account on the basis of the evidence already seen) firms conduct or take additional steps to confirm the control and ownership of the business after the account has been opened, by checking to ensure directorships have been updated. Where mitigating steps have been taken to compensate for information not being easily available, firms should consider the probability that additional monitoring of the customer’s transactions and activity should be put in place.

16.32.33 A firm must be reasonably satisfied that the persons starting up the business are who they said they are, and are associated with the firm. Reasonable steps must be taken to verify the identity of the persons setting up a new business, as well as any beneficial owners, which may often be based on electronic checks. In the majority of cases, the individuals starting up a business are likely to be its beneficial owners. A check of the amount of capital invested in the business, whether it is in line with the firm’s knowledge of the individual(s) and whether it seems in line with their age/experience, etc., may be a pointer to whether further enquiries need to be made about other possible beneficial owners.

16.33.34 Wherever possible, documentation of the firm’s business address should be obtained. Where the firm can plausibly argue that this is not possible because it is in the early stages of start-up, the address of the firm should be verified later; in the interim, the bank may wish to obtain evidence of the address(es) of the person(s) starting up the business. In certain circumstances, a visit to the place of business may be helpful to confirm the existence and activities of the business.

16.34.35 In determining the identification appropriate for partnerships (see Part I, paragraphs 5.177 - 5.191), whose structure and business may vary considerably, and will include professional firms e.g. solicitors, accountants, as well as less regulated businesses, it will be important to ascertain where control of the business lies, and to take account of the risk inherent in the nature of the business.
Enhanced due diligence

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

➢ When the business, or other aspect, of the customer relationship is determined to present a high risk of money laundering or terrorist financing. Examples should be set out in the firm’s risk-based approach and should reflect the firm’s own experience and information produced by the authorities. See Part I, paragraphs 4.39 – 4.69 and section 5.5 for general guidance.

➢ When the proposed customer relationship or transaction is with a person established in a high risk non-EEA country;

➢ When establishing a correspondent relationship with an institution in a non-EEA state (although in practice most firms would not regard such relationships as forming part of their ‘retail’ business).

➢ When the applicant is a PEP, or a family member or close associate of a PEP. See Part I, paragraphs 5.5.1 – 5.5.31.

➢ Where a customer has provided false or stolen identification documentation or information on establishing a relationship;

➢ Where:
  o A transaction is complex and unusually large, or
  o There is an unusual pattern of transactions, and
The transaction has no apparent economic or legal purpose.

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

➢ High cash turnover businesses: casinos, bars, clubs, taxi firms, launderettes, takeaway restaurants

➢ Money service businesses: cheque encashment agencies, bureaux de change, money transmitters

➢ Gaming and gambling businesses

➢ Computer/high technology/telecom/mobile phone sales and distribution, noting especially the high propensity of this sector to VAT ‘Carousel’ fraud

➢ Companies registered in one offshore jurisdiction as a non-resident company with no local operations but managed out of another, or where a company is registered in a high risk jurisdiction, or where beneficial owners with significant interests in the company are resident in a high risk jurisdiction

➢ Unregistered charities based or headquartered outside the UK, ‘foundations’, cultural associations and the like, particularly if centred on certain target groups, including specific ethnic communities, whether based in or outside the UK (see FATF Typologies Report 2003/4 under ‘Non-profit organisations’ – at www.fatf-gafi.org)

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

Financial exclusion
Denying those who are financially excluded from access to the financial sector is an issue for deposit takers. Reference should be made to the guidance given in Part I, paragraphs 5.3.121 to 5.3.125, and Annex 1-I.

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.

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.

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.

Firms should note the guidance contained in Part I, section 5.7, and the examples of higher risk businesses in paragraph 1.37. It is likely that in significant retail banking operations, some form of automated monitoring of customer transactions and activity will be required. However, staff vigilance is also essential, in order to identify counter transactions in particular that may represent money laundering, and in order to ensure prompt reporting of initial suspicions, and application for consent where this is required.

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.

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.

In a volume business, compliance with the identification requirements set out in the firm’s policies and procedures should also be closely monitored. The percentage failure rate in such compliance should be low, probably not exceeding low single figures. Repeated failures in excess of this level by a firm over a period of time may point to a systemic weakness in its identification procedures which, if not corrected, would be a potential breach of FCA Rules and should be reported to senior management. This should be part of the standard management information that a firm collates and provides to MLRO and other senior management.

Training
16.46 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

16.47 Firms should note the guidance contained in Part I, Chapter 6. As indicated in Part I, paragraphs 7.32 to 7.40, further reference material and typologies are available from the external sources cited, viz: FATF and NCA websites. In addition, firms should be aware of the requirement under Section 331(4) of the Proceeds of Crime Act for reports to be submitted “as soon as practicable” to NCA.

16.48 There is no formal definition of what “as soon as practicable” means, but firms should note the enforcement action taken by the FCA in respect of the anti money laundering procedures in place at a large UK firm. The FCA imposed a financial penalty on the firm due, in part, to finding that over half of the firm’s suspicious activity reports were submitted to NCA more than 30 days after having been reported internally to the firm’s nominated officer. In view of the volumes of reports which may be generated in this sector, firms may wish to keep under review whether their nominated officer function is adequately resourced. It is reasonable to base the timescale not on the date that an alert is generated but rather the point in time at which, following internal investigation, a determination is made that it is suspicious and should be reported to NCA. In all circumstances, however, firms should ensure that their end to end process is as efficient as it can be.

Interbank Agency Agreements

16.49 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 an Interbank Agency Agreement, which permits participating banks to service other banks’ customers. In such a case, a report should be made to the nominated officer of firm A, who may alert the nominated officer of firm B. In each case, the nominated officer will need to form their own judgement whether to disclose the circumstances to NCA.
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:

<table>
<thead>
<tr>
<th>Customer</th>
<th>Document(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefit claimants</td>
<td>Entitlement letter issued by DWP, HMRC or local authority, or Identity Confirmation Letter issued by DWP or local authority</td>
</tr>
<tr>
<td>Those in care homes/sheltered accommodation/refuge</td>
<td>Letter from care home manager/warden of sheltered accommodation or refuge</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Those on probation</td>
<td>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.</td>
</tr>
<tr>
<td>International students</td>
<td>Passport or EEA National Identity Card AND Letter of Acceptance or Letter of Introduction from Institution on the UK Border Agency list (see <a href="http://www.bia.homeoffice.gov.uk/employers/points/">http://www.bia.homeoffice.gov.uk/employers/points/</a>). See the pro forma agreed for this purpose with UKCOSA: The Council for International Education, attached as Annex 1-II. See also Part I, paragraphs 5.3.118-119.</td>
</tr>
<tr>
<td>Prisoners</td>
<td>It may be possible to apply standard identification procedures. Otherwise, a letter from the governor of the prison, or, if the applicant has been released, from a police or probation officer or hostel manager would normally be sufficient. See the pro forma agreed for this purpose with the National Offender Management Service and UNLOCK, attached as Annex 1-III</td>
</tr>
<tr>
<td>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)</td>
<td>National Passport, or National Identity Card (nationals of EEA and Switzerland)</td>
</tr>
</tbody>
</table>

Details of documents required by migrant workers are available at www.employingmigrants.org.uk, and Home Office website https://www.gov.uk/government/organisations/home-office. Firms are not required to establish whether an applicant is legally entitled to work in the UK but if, in the course of checking identity, it came to light that the applicant was not
entitled to do so, the deposit of earnings from employment could constitute an arrangement under the Proceeds of Crime Act.

<table>
<thead>
<tr>
<th>Refugees (those who are not on benefit)</th>
<th>Immigration Status Document with <strong>Biometric</strong> Residence Permit, or IND travel document (i.e., Blue Convention Travel doc, or Red Stateless Persons doc, or Brown Certificate of Identity doc)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

| Asylum seekers | IND Application Registration Card (ARC)  
**NB This document shows the status of the individual, and does not confirm their identity** |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

| 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 6.3.7 (5) (G) “not unreasonably [to] deny access to its service to potential customers who cannot reasonably be expected to provide detailed evidence of identity.”
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………………………………………….
PERSONAL IDENTIFICATION DOCUMENT

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

Name……………………………………………….
Nationality ……………………………………. Place of Birth……………..
Signature………………………………………… Date…………………….

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

…………………………………………………………………………………………
…………………………………………………………………………………………
Witnessed by

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

…………………………………………………………………………………………
Signature of witness

…………………………………………………………………………………………
The following sections must be signed by an authorised manager

Applicant’s Full Name

Applicant’s Date of Birth

Applicant’s Current Address (HMP/YOI)

Applicant’s Photograph (to be affixed here)

Expected Release Date

Address immediately prior to custody

Verification of name and address by HMP

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

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

Name

e-mail address

Direct telephone line

Signature

Date
Overview of the sector

1A.1 The MSB industry is extremely diverse, ranging from large international companies with numerous outlets worldwide to small, independent convenience stores in communities with population concentrations that do not necessarily have access to traditional banking services or in areas where English is rarely spoken.

1A.2 The range of products and services offered, and the customer bases served by MSBs, are equally diverse. Indeed, while they all fall under the definition of a money services business, the types of businesses are quite distinct. Some MSBs offer a variety of services, whilst others only offer money services as an ancillary component to their primary business, such as a convenience store that cashes cheques or a hotel that provides currency exchange.

1A.3 MSB services can include one or more of the following activities:

➢ Currency dealing/exchanging;
➢ Cheque cashing;
➢ Money remitting; and
➢ Issuing, selling and redeeming stored value and monetary instruments, such as money orders and traveller’s cheques.

1A.4 Under the ML Regulations, MSBs are required to register with HMRC in order to be able to carry out their activities, unless they are subject to FCA supervision. Registration is subject to the MSB meeting the ‘fit and proper’ test set out in the ML Regulations, which from 26 June 2017 is also applied to an MSB’s agents.

1A.5 Where MSBs carry out money transmission services, they are included within the definition of financial institutions, and are therefore subject to the full provisions of the ML Regulations. The exemption from the ML Regulations for activities that are engaged in only on an occasional or very limited basis does not apply to money transmission services.

1A.6 Under the Payment Services Regulations 2009, MSBs carrying out money remittance services must be included on a register maintained by the FCA. MSBs on the register can be:

• Authorised Payment Institutions (which are required to meet certain minimum standards in respect of capital, management and systems and controls, and whose client funds must be kept in a separate client account with an authorised bank); or
• Small Payment Institutions (which are exempt from minimum capital requirements, but whose management must meet certain requirements on propriety and experience, and whose business level must be less than a prescribed monthly maximum); or
Agents of an API or an SPI.

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

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

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

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

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

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

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

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

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

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

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

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

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

Risk assessment

1A.16 The risk inherent in the MSB sector is not the nature of the sector itself, but the potential for the abuse of the sector by criminals. It is therefore important that firms understand these potential risks, and manage them effectively. This risk will be greater in some MSBs than in others, and firms should be able to carry out a risk assessment that allows such a judgement to be made.

1A.17 As a part of a risk-based approach, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers’ beneficial owners, for two principal reasons:

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

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

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

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

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

- **Types of products and services offered**
  
  In order to assess risks, firms should know the categories of money services engaged in by the particular MSB customer.

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

- **Location(s) and market(s) served**
  
  Money laundering risks within an MSB can vary widely depending on the locations, customer bases, and markets served. Relevant considerations include whether markets served are domestic or international, or whether services are targeted to local residents or to broad markets. For example, a convenience store that only cashes payroll or government cheques generally presents a lower money
laundering risk than a cheque casher that cashes any type of third-party cheque or cashes cheques for commercial enterprises (which generally involve larger amounts).

➢ Anticipated account activity

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

➢ Purpose of the account

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

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

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

Customer due diligence

About the customer

Regulation 5(c)

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

1A.25 It is important to know and understand any associations the MSB may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc.) and the individuals who may influence its operations (political connections, etc.). A visit to the place of business may be helpful to confirm the existence and activities of the entity.
Regulation 5(b)

1A.26 In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm’s objective must be to know who has ownership or control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds.

Regulation 6(1)  Regulation 5(b)

1A.27 As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the MSB’s shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. The firm must take risk based and adequate measures to verify the identity of those individuals (see Part I, paragraphs 5.3.11 and 5.3.12). Verifying the identity of the beneficial owner(s) will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

1A.28 Following the firm’s assessment of the money laundering or terrorist financing risk presented by the MSB, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals (Part I, paragraphs 5.3.57 to 5.3.105). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other directors. Firms may, of course, already be required to identify a particular director as a beneficial owner if the director owns or controls more than 25% of the company’s shares or voting rights (see Part I, paragraph 5.3.126).

1A.29 Part I, paragraphs 5.3.129 – 5.3.132 refer to the standard evidence for corporate customers, and Part I, paragraphs 5.3.133 – 5.3.139 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Nature and purpose of the relationship

1A.30 A firm must understand the purpose and intended nature of the business relationship to assess whether the proposed business relationship is in line with the firm’s expectation and to provide the firm with a meaningful basis for on-going monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

1A.31 Depending on the firm’s risk assessment of the situation, information that might be relevant may include some or all of the following:

- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- the origin of the initial and on-going source(s) of wealth and funds of the MSB;
- copies of recent and current financial statements;
the various relationships between signatories and with underlying beneficial owners;

➢ the anticipated level and nature of the activity that is to be undertaken through the relationship, on each account to be opened;

➢ the MSB’s settlement arrangements, including the relationship with parties in the second and third miles.

1A.32 In the light of the risk it perceives in the proposed customer, a firm may include consideration of matters such as:

➢ its public disciplinary record, to the extent that this is available;

➢ the nature of the customer, the product/service sought and the sums involved;

➢ any adverse experience of the other firm’s general efficiency in business dealings;

➢ any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

MSB’s AML/CTF policies

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

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

Enhanced due diligence (EDD)

Regulation 14(1)(b) 1A.35 A firm’s due diligence should be commensurate with the level of risk of the MSB customer identified through its risk assessment. If a firm’s risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be required to conduct further due diligence in a manner commensurate with the heightened risk.

1A.36 Whenever faced with less transparency or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers.
While the extent to which firms should perform further due diligence beyond the minimum will be dictated by the level of risk posed by the particular customer, it is not the case that all MSBs will always require additional due diligence. In some cases, no further customer due diligence will be required - in other situations, however, the further due diligence required may be extensive. In all cases, the level of due diligence applied will be dictated by the risks associated with the particular customer.

Depending on the level of perceived risk, and the size and sophistication of the particular MSB, firms may pursue a range of actions as part of an appropriate due diligence review or risk management assessment of an MSB seeking to establish an account relationship. Similarly, if the firm becomes aware of changes in the profile of the MSB to which services are being provided, additional steps may be appropriate. Firms will not uniformly require any or all of the actions identified for all MSB customers.

Where the customer is an overseas, unregulated MSB (see 1A.42 if a UK MSB), additional due diligence should be undertaken to ascertain and assess the effectiveness of the MSB’s internal policy on money laundering/terrorist financing prevention and its CDD and activity monitoring controls and procedures. In larger cases, where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to UK or equivalent standards. If not, the extent to which the parent’s controls meet UK or equivalent standards, and whether these are communicated and enforced ‘effectively’ throughout its network of international offices, should be ascertained.

Where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service provided, request additional information, for example as to the MSB’s activities, customer base or ownership, in order to decide whether to continue with the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of higher-risk business relationships.

On-going monitoring

Firms are required to conduct on-going monitoring of business relationships, and to identify and report known or suspected suspicious activity or transactions. Risk-based monitoring of accounts maintained for all customers, including MSBs, is a key element of an effective system to identify and, where appropriate, report suspicious activity. The level and frequency of such monitoring will depend, among other things, on the firm’s risk assessment and the activity across the account. The firm may require that a regular (or periodic) audit or review of the MSB’s AML/CTF controls is carried out.

Based on the firm’s assessment of the risks of its particular MSB customer, monitoring should include periodic confirmation that initial
projections of account activity have remained reasonably consistent over time. The mere existence of unusual transactions does not necessarily mean that a problem exists, but may be an indication that additional review is necessary. Furthermore, risk-based monitoring generally does not include “real-time” monitoring of all transactions flowing through the account of an MSB, such as a review of the payee or drawer of every deposited cheque.

1A.43 Examples of unusual activity across MSB accounts, that may or may not be potentially suspicious generally involving significant unexplained variations in transaction size, nature, or frequency through the account, could include:

➢ A cheque casher depositing cheques from financial institutions in jurisdictions posing heightened risk for money laundering or the financing of terrorism or from countries identified as having weak anti-money laundering controls when the MSB does not overtly market to individuals related to the particular jurisdiction;

➢ A cheque casher seeking to deposit currency. Given that a cheque casher would typically deposit cheques and withdraw currency to meet its business needs, any deposits of currency may be an indicator of suspicious activity;

➢ A money transmitter transferring funds to a different jurisdiction from expected based on the due diligence information that the firm had assessed for the particular money services business. For example, if the money transmitter represented to the firm or in its business plan that it specializes in remittances to Latin America and starts transmitting funds on a regular basis to another part of the world, the unexplained change in business practices may be indicative of suspicious activity; or

➢ A money transmitter or seller/issuer of money ordering deposits currency significantly in excess of expected amounts, based on the due diligence information that the firm had assessed for the particular MSB, without any justifiable explanation, such as an expansion of business activity, new locations, etc.

1A.44 Given the importance of the requirement for MSBs to register, a firm should file a suspicious activity report if it becomes aware that an MSB is operating without registration with HMRC, or authorisation by the FCA.

1A.45 There is no requirement in the ML Regulations that a firm must close an account that is the subject of a suspicious activity report. Firms are therefore not expected automatically to terminate existing accounts of MSBs based solely on the discovery that the customer is an MSB that has failed to comply with registration requirements (although continuing non-compliance by the MSB may be an indicator of heightened risk). In these circumstances, further enquiries ought to be made.
ANNEX 1A-1

RISK INDICATORS

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

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

Examples of potentially lower risk indicator:

The MSB –

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

Examples of potentially higher risk indicator:

The MSB –

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

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

Overview of the sector

2.1 A credit card evidences an unsecured borrowing arrangement between an issuing entity and a cardholder, whereby the cardholder obtains goods and services through merchants approved by the Merchant Acquirer (see paragraph 2.9), up to an agreed credit limit on the card. Cards may also be used at ATMs to withdraw cash, which is then added to the balance owing on the card account. Withdrawals (charged to the card account) across a bank counter may be made, upon the presentation of sufficient evidence of identity.

2.2 The cardholder agrees to repay any borrowing, in full or in part, at the end of each statement period. There will be a minimum monthly repayment figure (typically between 2% and 3% of the outstanding balance, depending on the issuer). Interest is charged by the issuing entity, at an agreed rate, on any borrowing not repaid at the end of each period. Any interest or fees charged are added to the card balance.

2.3 Cards are issued by individual Card Issuers, each of whom is a member of one or more Card Schemes (e.g., Visa, MasterCard). Each credit card will be branded with the logo of one of the card schemes, and may be used at any merchant worldwide that displays that particular scheme logo. Cash may also be withdrawn through ATMs which bear the scheme logo.

2.4 Credit cards may be used through a number of channels. They may be used at merchants’ premises at the point of sale, or may be used remotely over the telephone, web or mail (referred to as ‘card not present’ use). In card not present use, additional security numbers shown on the card may or may not be required to be used, depending on the agreement between merchant and its acquiring bank. The Merchant Acquirer (see paragraph 2.9) will undertake its own assessment of the merchant, and decide what type of delivery channel(s) it will allow the merchant to use to accept card transactions.

Different types of credit card

2.5 A Card Issuer may have a direct relationship with the cardholder, in which case the card will clearly indicate the names of the Issuer and of the cardholder. Some Issuers also issue and manage cards branded in the name of other firms (referred to as ‘branded cards’), and/or which carry the name of another organisation (referred to as ‘affinity cards’). Each card scheme has strict rules about the names that must appear on the face of each card.

2.6 Store cards are similar to credit cards, but are issued in the name of a retail organisation, which is not a member of a card scheme. These cards may be issued and operated by a regulated entity within the store group, or on their behalf by other firms that issue and operate other cards. Store cards may only be used in branches of the store, or in associated organisations, and not in other outlets. Generally, store cards cannot be used to obtain cash. They are therefore limited to the domestic market, and cannot be used internationally.

2.7 As well as issuing cards to individuals, an Issuer may provide cards to corporate organisations, where a number of separate cards are provided for use by nominated employees of that organisation. The corporate entity generally carries the liability for the borrowings accrued under their employees’ use of their cards, although in some cases the company places the
primary liability for repayment on the employee (generally to encourage the employee to account for his expenses, and to claim reimbursement from the company, in a timely manner).

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

Merchant acquisition

2.9 Merchant Acquirers provide a payment card processing service, which facilitates acceptance of payment card transactions between cardholders and merchants. Payment cards that bear card scheme acceptance brands (e.g., MasterCard and Visa) are issued by banks and financial institutions which are members of the relevant card scheme. The Merchant Acquirer processes the card transaction on behalf of its merchant customer, including, in appropriate cases, seeking authorisation for the transaction from the card issuer.

2.10 Payment (settlement) is made by the Card Issuer through the Card Scheme – e.g., Visa. In turn the scheme will pass funds to the Merchant Acquirer through the merchant’s bank account. The merchant is therefore a customer of (i) the acquiring bank for the purposes of transaction processing, and (ii) the bank with which it maintains its primary banking relationship, which may or may not be the same as the acquirer. The merchant does not have a relationship with the Card Issuer. For further guidance on transactions through Merchant Acquirers, see Part III, sector 1: Transparency in electronic payments, paragraph 1.18.

2.11 At the outset of the relationship with the merchant, the Merchant Acquirer will gather information on such matters as the expected card turnover, and average ticket value. This information is assessed in respect to the type of business the merchant is undertaking and the size of such business.

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

2.12 Credit cards are a way of obtaining unsecured borrowing. As such, the initial risks are more related to fraud than to ‘classic’ money laundering; but handling the criminal property arising as a result of fraud is also money laundering. Card Issuers will therefore generally carry out some degree of credit check before accepting applications.

2.13 The money laundering risk relates largely to the source and means by which repayment of the borrowing on the card is made. Payments may also be made by third parties. Such third party payments, especially if they are in cash or by debit cards from different locations or accounts, represent a higher level of money laundering risk than when they come from the cardholder's bank account by means of cheque or direct debit.

2.14 Balances on cards may move into credit, if cardholders repay too much, or where merchants pass credits/refunds across an account. Customers may ask for a refund of their credit balance. Issuance of a cheque by a Card Issuer can facilitate money laundering, as a credit balance made up of illicit funds could thereby be passed off as legitimate funds coming from a regulated firm.

2.15 Where a cardholder uses his card for gambling purposes (although the use of credit cards is prohibited in casinos), a card balance can easily be in credit, as scheme rules require that winnings are credited to the card used for the bet. It can be difficult in such circumstances to identify an unusual pattern of activity, as a fluctuating balance would be a legitimate profile for such a cardholder.
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 no longer be able to undertake enhanced due diligence on the basis of the details that it known to it about the cardholder. Such steps might include ascertaining:

- whether the primary or any secondary cardholder (including corporate cardholders) is resident in a high-risk jurisdiction or, for example, a country identified in relevant corruption or risk indices (such as Transparency International’s Corruption Perception Index) as having a high level of corruption
- whether any primary or secondary cardholder is a politically exposed person and, if so, the nature and extent of any money laundering/terrorist financing risk associated with them. More full guidance on the treatment of PEPs is provided in Part I, section 5.5 of this guidance.

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
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 5.3.112.
2.28 The standard verification requirement set out in Part I, Chapter 5 should be applied, as appropriate, to credit card and store card holders, although ascertaining the purpose of the account, and the expected flow of funds, would not be appropriate for such cards.

2.29 A risk-based approach to verifying the identity of secondary cardholders should be carried out as follows:

➢ The standard information set out in Part I, paragraph 5.3.59 should be collected for all secondary cardholders and recorded in such a way that the data are readily searchable.

➢ Firms should assess the extent to which they should verify any of the data so obtained, in accordance with the guidance set out in Part I, paragraph 5.3.60, from independent documentary or electronic evidence, in the light of their aggregate controls designed to mitigate fraud and money laundering risks, and bearing in mind the extent to which the firm applies the risk controls set out in paragraph 2.18. However, there is a presumption that such verification will be carried out, other than in the following circumstances.

2.22  In the case of store cards, because of the restrictions on their use, see paragraph 2.6.

2.23  In the case of commercial cards, because of the restrictions on their issue, see paragraph 2.7, although a firm’s risk-based approach may deem it prudent to verify employee cardholders of their smaller commercial card customers.

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

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

2.30 In relation to branded and affinity cards, where another regulated firm has the primary relationship with the cardholder, the partner organisation would need to undertake that it holds information on the applicant, and that this information would be supplied to the card issuer if requested.

2.31 In respect of a merchant, the Merchant Acquirer should apply the standard verification requirement in Part I, Chapter 5, adjusted as necessary to take account of the activities in which the merchant is engaged, turnover levels, the sophistication of available monitoring tools to identify any fraudulent history, as well as transaction activity, and the location of the bank account over which transactions are settled.

2.32 Where functions in relation to card issuing, especially initial customer due diligence, is outsourced, the firm should have regard to the FCA’s guidance on outsourcing (www.fsa.co.uk/html/handbook/SYSC/8). In particular, Card Issuers should have criteria in place for assessing, initially and on an ongoing basis, the extent and robustness of the systems and procedures (of the firm to which the function is outsourced) for carrying out customer identification.
2.33 It would be unusual for a Card Issuer to revisit the information held in respect of a cardholder. Credit cards are primarily a distance transaction process. An account is opened (after due diligence checks are completed), a balance is acquired, a bill sent and payment received. This cycle is repeated until card closure and the majority of cardholders rarely, if ever, contact the Card Issuer.

*Enhanced due diligence*

2.34 An issuer should have criteria and procedures in place for identifying higher risk customers. Such customers must be subject to enhanced due diligence. This applies in the case of customers identified as being PEPs, or who are resident in high-risk and/or non FATF jurisdictions.

2.35 Firms’ procedures should include how customers should be dealt with, depending on the risk identified. Where necessary and appropriate, reference to a senior member of staff should be made in unusual circumstances. This will include getting senior manager approval for relationships with PEPs, although the level of seniority will depend on the level of risk represented by the PEP concerned.

*Monitoring*

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

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

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

Introduction

What is electronic money?

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

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

(a) is issued on receipt of funds for the purpose of making payment transactions;
(b) is accepted by a person other than the electronic money issuer; and
(c) is not excluded by regulation 3.'

3.2. Regulation 3 of the Electronic Money Regulations 2011 states that electronic money does not include:

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

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

(b) monetary value that is used to make payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.'

3.3. Electronic money is therefore a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities. It may be a card-based, voucher-based, mobile app-based or an online account-based product.

3.4. The Electronic Money Regulations 2011 also provide for a number of exemptions (see para. 3.2 above). Where such products are exempt from financial services regulation, they are also likely to fall outside of the scope of the AML and CTF regulation. Issuers must, however, examine such products on a case-by-case basis to identify whether such regulation continues to apply.

3.5. Electronic money may be issued by banks or building societies with the requisite variation of permission from the FCA, or it may be issued by specialist electronic money institutions, who obtain an authorisation from the FCA under the Electronic Money Regulations 2011 (for other persons also permitted to issue electronic money, such as local authorities, see Regulation 2(1))
of the Electronic Money Regulations 2011.) Where electronic money institutions meet the
conditions set out in Regulation 13 of the Electronic Money Regulations 2011, they may
register with the FCA as small electronic money institutions.

3.6. All issuers of electronic money are subject to the Money Laundering Regulations 2017, the
Terrorism Act 2000, the Anti-terrorism, Crime and Security Act 2001, the Wire Transfer
They must also comply with the legislation implementing the UK’s financial sanctions regime.
Issuers of electronic money that are FSMA-authorised persons (i.e. banks and building
societies) must also comply with relevant provisions in the FCA’s handbook for AML/CTF
purposes.

3.7. Electronic money may also be issued into the UK by EEA credit and financial institutions
holding the appropriate passport from their home state competent authority under Art. 25 or 28
of the Banking Consolidation Directive (2006/48/EC) or Arts. 28 and 29 of the Payment
Services Directive (EU) 2015/2366 by virtue of Art. 3(1) of the Electronic Money Directive
(2009/110/EC). Where such issuance, distribution or redemption is on a cross-border services
basis, i.e. without an establishment in the UK, the issuer’s AML procedures are regulated by
the home state authorities, but issuers must be aware that in some cases, UK legislation may
extend to such providers of services. UK AML/CTF legislation will apply where the service is
provided through an establishment in the UK.

Definitions

3.8. The following terms are used in this guidance:

c. Card-based products:

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

c. Electronic Money Association (EMA):

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

c. Merchant:

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

c. Mobile app-based products:

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

c. Online account-based products:

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

c. Payment Service Provider (PSP):

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

c. Purse:

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

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

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

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

**Voucher-based products:**

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

**Wire Transfer Regulation (WTR):**

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

---

**Notes**

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

**Money laundering and terrorist financing risks related to electronic money**

3.10. Electronic money is a retail payment product that is used predominantly for making small value payments. It is susceptible to the same risks of money laundering and terrorist financing as other retail payment products. In the absence of AML systems and controls, there is a significant risk of money laundering taking place. The implementation of AML systems and controls and certain product design features can contribute to mitigating this risk.

3.11. Furthermore, where electronic money is limited to small value payments, its use is less attractive to would-be launderers. For terrorist financing and other financial crime, electronic money offers a more accountable, and therefore less attractive means of transferring money compared to cash.

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

3.13. As issuers of electronic money usually occupy the position of intermediaries in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement that complements identity data provided by other financial institutions. This may be equally or more valuable evidence than a repetition of the verification of identity process.
3.14. Fraud prevention and consumer protection concerns lead to the placement of transaction, turnover and purse limits on products, limiting the risk to both issuer and consumer. These limits act to restrict the usefulness of the product for money laundering, and make unusual transactions more detectable.

3.15. A non-exhaustive list of risk factors that may apply to electronic money products is given in para. 3.18 below; risk mitigating factors are listed in para. 3.20 below. Other risks set out in the draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities and in Part I, Annex 4-II of this guidance also affect issuers, and issuers should consider these as part of the risk assessment that they undertake. Issuers should in particular be alert to emerging information on financial crime risks specific to electronic money, such as those highlighted by

1. Their own transaction monitoring processes;
2. The FCA;
3. The NCA;
4. National and supra-national risk assessments and associated recommendations;
5. The Joint Committee of the European Supervisory Authorities;
6. The European Commission (EC list of high-risk third countries); and
7. Typology reports, such as those from the EMA and the FATF.

3.16. The overall ML/TF risk posed by an electronic money product is a function of its design, its use, and the issuer’s AML/CTF controls. The overall risk posed is the outcome of competing factors, not any single feature of the product.1

3.17. Issuers will need to put in place risk management processes appropriate to the size and nature of their business and must evidence that they deploy an adequate range of controls to mitigate the ML/TF risks they encounter.

Risk factors

3.18. The following factors will increase the risk of electronic money products being used for money laundering or terrorist financing (for ways in which this risk can be mitigated by applying controls or by other means, see para. 3.21 below):

• High, or no transaction or purse limits. The higher the value and frequency of transactions, and the higher the purse limit, the greater the risk, particularly where compared to anticipated usage, or where customers are permitted to hold multiple purses; the €15,000 threshold for occasional transactions provided in the Money Laundering Regulations 2017 may in this context provide a convenient comparator when assessing such risk;

• The ability to conduct frequent cross-border transactions, although the risk may be less within 3-party schemes that afford the issuer oversight over both payer and payee unless within a single scheme, can give rise to difficulties with information sharing. Dependence on counterparty systems increases the risk;

---

1 The draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities, paras. 31-32, state: “Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of money laundering and terrorist financing risk associated with a business relationship or occasional transaction. As part of this assessment, firms may decide to weigh factors differently depending on their relative importance.”
• E-money issuers can use complex business models such as using programme managers to ‘white label’ their products, this can result in a weakening of the complex control environment and therefore in a higher risk that a particular product could be used for ML/TF;

• Some merchant activity, such as betting and gaming, poses a higher risk of money laundering. This is because of the higher amounts of funds that are transacted and because of the opportunities presented within the merchant environment;

• Funding of purses by unverified parties presents a higher risk of money laundering, whether it is the customer who is unverified or a third party;

• Funding of purses using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering;

• The non-face-to-face nature of many products gives rise to increased risk;

• The ability of consumers to hold multiple purses (for example open multiple accounts or purchase a number of cards) without verification of identity increases the risk;

• Cash access, for example by way of ATMs, as well as an allowance for the payment of refunds in cash for purchases made using electronic money, will increase the risk;

• Increased product functionality may in some instances give rise to higher risk of money laundering (product functionality includes person-to-business, person-to-person, and business-to-business transfers);

• Products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the customer is able to pass on linked ‘partner’ cards to anonymous third parties;

• Segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk;

• The technology adopted by the product may give rise to specific risks that should be assessed.

3.1.9. Absence of any of the above factors will decrease the risk.

Risk mitigating factors

3.20. Electronic money issuers address the risks that are inherent in payments in a similar manner to other retail payment products by putting in place systems and controls that prevent money laundering and terrorist financing by detecting unusual transactions and predetermined patterns of activity.

3.21. The systems and controls issuers put in place must be commensurate to the money laundering and terrorist financing risk they are exposed to. The detail of issuers’ systems and controls will therefore vary. Examples include those that:

• Strong oversight of outsourced functions;

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

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

For transfers subject to the Regulation, see the requirements for up-front verification where transfers are paid out in cash or electronic money in Article 7(4)(a).
• Place limits on purse storage values, cumulative turnover or amounts transacted;
• Can detect money laundering transaction patterns, including those described in the EMA or similar typologies documents;
• Will detect anomalies to normal transaction patterns;
• Can identify multiple purses held by a single individual or group of individuals, such as the holding of multiple accounts or the ‘stockpiling’ of pre-paid cards;
• Can look for indicators of accounts being opened with different issuers as well as attempts to pool funds from different sources;
• Can identify discrepancies between submitted and detected information, for example, between country of origin submitted information and the electronically-detected IP address, geo-location information or device-related information;
• Deploy sufficient resources to address money laundering risks, including, where necessary, specialist expertise for the detection of suspicious activity;
• Allow collaboration with merchants that accept electronic money to identify and prevent suspicious activity;
• Restrict funding of electronic money products to funds drawn on accounts held at credit and financial institutions in the UK, the EU or a comparable jurisdiction, and allow redemption of electronic money only into accounts held at such institutions.

Customer Due Diligence

3.22. The Money Laundering Regulations 2017 require firms to apply customer due diligence measures on a risk-sensitive basis. Customer due diligence measures comprise the identification and verification of the customer’s (and, where applicable, the beneficial owner’s) identity and obtaining information on the purpose and intended nature of the business relationship or transaction. There is also a requirement for the ongoing monitoring of the business relationship. Part I, Chapter 5 sets out how firms can meet these requirements.

3.23. Detailed guidance for verifying the identity of customers who do not have access to a bank account, or who lack credit or financial history, is provided under the financial exclusion provisions of Part I, paras. 5.3.108 to 5.3.125.

3.24. Issuers will also need to satisfy themselves that they comply with sanctions legislation. Guidance on this is provided throughout Part I and in Part III, section 4.

Verification of identity – consumers

3.25. Taking account of the risk mitigation features applied to electronic money systems, the approach to undertaking customer due diligence in the electronic money sector is predicated on the need to minimise barriers to take-up of the products, whilst addressing the risk of money laundering and meeting the obligations set out in the Money Laundering Regulations 2017.

3.26. In addition to normal customer due diligence, the Money Laundering Regulations 2017 specify the following exemptions and allowances in relation to customer due diligence:

• The e-money-specific exemption: Circumstances where an exemption from the requirement to apply customer due diligence measures may be applied. A purse must meet specific functionality, storage, turnover and redemption restrictions in order to qualify for the e-money-specific exemption (see paras. 3.30 to 3.34 below), and issuers must have systems and controls in place to make sure these restrictions are not breached.
• Simplified due diligence: Circumstances where simplified due diligence may be applied. The allowance to apply simplified due diligence is risk-based, and parameters will differ between products. Where the product is no longer low risk, where the issuer doubts the veracity or accuracy of documents or information previously obtained, or where the issuer suspects money laundering or terrorist financing, customer due diligence and, where appropriate, enhanced due diligence measures must be applied.

3.27. Monitoring of the business relationship and transactions must be undertaken during the application of both the e-money-specific exemption and simplified due diligence. Issuers should also comply with the requirements set out in paras. 3.46 to 3.49 below.

3.28. Issuers, in common with other financial services providers, are required to verify identity of the customer at the outset of a business relationship. The e-money-specific exemption and simplified due diligence enable issuers to postpone the verification of identity until the exemption limits have been reached. Issuers making use of these provisions whose electronic money products may at some point exceed these limits should have in place systems to anticipate when a customer approaches the exemption limits. Where there is an obligation to undertake customer due diligence and this cannot be discharged, issuers must freeze the account pending the provision of the required information.

3.29. Enhanced due diligence is required in circumstances giving rise to an overall higher risk. The extent of enhanced due diligence measures required will depend on the level of risk a situation presents (see paras. 3.50 to 3.53 below).

The e-money-specific exemption

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

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

(a) the maximum amount which can be stored electronically is 250 euros or (if the amount stored can only be used within the United Kingdom), 500 euros;

(b) the payment instrument used in connection with the electronic money (“the relevant payment instrument”) is—

i) not reloadable, or

ii) is subject to a maximum limit on monthly payment transactions of 250 euros which can only be used within the United Kingdom;

(c) the relevant payment instrument is used exclusively to purchase goods or services;

(d) anonymous electronic money cannot be added to the relevant payment instrument unless the source of that money is known.

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

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

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

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

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

Non-reloadable purses

3.31. Electronic money purses that cannot be recharged may benefit from the e-money-specific exemption if:

- The purse limit is restricted to €250 (or €500 if the amount stored can only be used within the United Kingdom);
- The instrument is used only for purchase transactions of goods and services;
- The device cannot be funded with anonymous e-money; and
- The customer does not seek to redeem more than €100 in cash in a single transaction and the cash withdrawal does not cause the purse limit to be exceeded.

3.32. Non-reloadable purses are often sold as gift cards. The purchase of multiple such products is sometimes expected, particularly during certain times of the year, and the risk of money laundering arising from multiple purchases is likely to remain low. Issuers should, however, adopt a maximum total value that they will allow single customers to purchase without carrying out customer due diligence measures. This total value can be determined on a risk weighted basis, but should not exceed €1,500.

Reloadable purses

3.33. Electronic money purses that can be recharged may benefit from the e-money-specific exemption if:

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

Simplified due diligence

3.34. Issuers may apply simplified due diligence measures in addition to the limits set by the e-money-specific exemption if business relationships or transactions present a low risk of money laundering or terrorist financing.
• 3.35. The assessment of low risk is based on the risk factors set out in Regulation 37(3) and 37(4). Regulation 18 also requires a relevant person to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business faces.

• 3.36. Simplified due diligence must always involve the identification and verification of the customer, but the extent of identification and verification can be varied depending on the risk, and verification may be postponed until the risk is no longer deemed to be low. In this case, issuers should set a reasonable threshold that will minimise potential abuse of the product.

• 3.37. Simplified due diligence may also involve verifying identity on the basis of fewer or less reliable sources, using alternative methods to verify identity, assuming the nature and intended purpose of the business relationship where this is obvious or reducing the intensity of monitoring.

Verification by reliance on the funding instrument under simplified due diligence

• 3.38. As part of a risk-based approach to verification of identity, the Money Laundering Regulations 2017 require that verification is carried out “on the basis of documents or information obtained from a reliable source which is independent of the customer.” In some cases, where the risk associated with the business relationship is low, a customer’s funding instrument (such as a credit card or bank account) can constitute such information, subject to the following additional requirements:

1a) The issuer remains ultimately responsible for meeting its customer due diligence obligations;

1b) The issuer has in place systems and processes for identifying incidents of fraudulent use of credit/debit cards and bank accounts;

1c) The issuer has in place systems and processes 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 steps must be undertaken;

1d) The issuer records and keeps records of relevant information, for example IP addresses, which assist in determining the electronic footprint of the customer, or where a POS terminal is used in a face-to-face environment, records the correct use of a PIN or other data;

1e) The funds to purchase electronic money are drawn from an account or credit card with, or issued by, a credit or financial institution in the UK, the EU or an equivalent jurisdiction, which is supervised for its AML controls;

1f) The issuer implements systems and controls to mitigate the risk of the funding card or account being itself subject to SDD;

2a) The issuer has reasonable evidence to conclude that the customer is the rightful holder of the account on which the funds are drawn (which may be achieved using the processes described in para. 3.41 below);

8. The overall amount transacted by one customer does not exceed a maximum turnover limit of €15,000 from the commencement of the business relationship.

Where the above are not satisfied, further customer due diligence measures have to be applied. Beyond this ceiling, issuers should set their own limit according to risk.

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

6 Other than a money service business, or a payment or electronic money institution providing mainly money remittance services.
• 3.39. A funding instrument on its own, however, is a weak form of verification of identity. The credit or financial institution whose evidence is being used may not have verified the customer to current standards, and there is a risk that the person using the account is not its rightful holder. This risk is even higher where an electronic money issuer has no evidence that the account is held in the same name as the customer, as is the case, for example, in relation to direct debits.

Establishing control over the funding instrument

• 3.40. Where payment is made electronically, it is usually not possible to verify the name of the account holder for the funding account. In this case, steps must be taken to establish that the customer is the rightful holder of the account from which the funds are drawn. These steps may include the following:

  • Micro-deposit. Some issuers have developed a means of establishing control over a funding account using a process that is convenient and effective. A small random amount of money is credited to a customer’s funding account and the customer is then required to discover the amount and to enter it on the issuer’s website. By entering the correct value, the customer demonstrates access to the bank/card statement or accounting system of their bank or financial institution. This method, and its close variants (such as the use of unique reference numbers), provides an acceptable means of confirming that the customer has access to the account, and therefore has control over it. It also provides a means of guarding against identity theft, contributing therefore to the verification of identity process. If such an approach is not used, some other means of establishing control of the account is needed.

  • Additional fraud checks. Issuers may also use additional fraud checks undertaken at the time of the transaction which seek to cross reference customer-submitted data against data held by the electronic money or card issuer or similar independent third party, and which gives the electronic money issuer the requisite level of confidence that the customer is the rightful holder of the card.

  • Evidence of legitimate use. Seeking evidence of legitimate use is an alternative to establishing formal control over an account. An account that is used to fund an electronic money purse over a significant period of time is more likely to be used legitimately, as the passage of time gives the rightful owner the opportunity to discover fraudulent use of the product and to block its use, which would in turn become evident to the issuer. Thus, for some products, this may provide a means of establishing legitimate use of a funding instrument. However:

    o 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.

    o A minimum period of four months must elapse, together with significant usage in terms of number and value of transactions over this time, to satisfy the issuer that the instrument is being legitimately used.⁷

• 3.41. Electronic money issuers must have processes in place to ensure that additional due diligence measures are applied if the money laundering and terrorist financing risk posed by the product or customer increases.

• 3.42. Information on the payer that is received as part of the obligations under the WTR may contribute to verifying a customer’s identity.

⁷ The four-month period should be completed before any limits associated with simplified due diligence are exceeded.
Basic requirements under this guidance in relation to products benefiting from the e-money-specific exemption and those applying simplified due diligence

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

Verification of identity

3.44. Either the electronic money system is a 3-party scheme; or it is a 4-party scheme, in which case all other participating issuers should ensure that the verification of identity and other due diligence measures carried out by that scheme in relation to merchants are, in the UK, equivalent to those of this sectoral guidance; or for other jurisdictions, are subject to equivalent requirements.

a) In all cases merchants must be subject to due diligence measures in accordance with Part I, Chapter 5 (but see para. 3.60 below for a limited exemption) or as required by an equivalent jurisdiction.

b) Where electronic money is accepted by merchants or other recipients belonging to a wider payment scheme (for example Visa or MasterCard), issuers must satisfy themselves that the verification of identity and other due diligence measures carried out by that scheme in relation to merchants are, in the UK, equivalent to those of this sectoral guidance; or for other jurisdictions, are subject to equivalent requirements.

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

Monitoring

3.45. Issuers must establish and maintain appropriate and risk-sensitive policies and procedures to monitor business relationships and transactions on an ongoing basis. Part I, Chapter 5 (see in particular section 5.7) sets out how this can be done.

3.46. If issuers wish to benefit from the e-money-specific exemption or the simplified due diligence provisions under this guidance, they must, in addition to the processes set out in Part I, Chapter 5, deploy specific minimum transaction monitoring and/or on-chip purse controls that enable control of the systems and recognition of suspicious activity. Such controls may include:

a) Transaction monitoring systems that detect anomalies or patterns of behaviour, or the unexpected use of the product, for example frequent cross-border transactions or withdrawals in products that were not designed for that purpose;

b) Systems that identify discrepancies between submitted and detected information – for example, between submitted country of origin information and the electronically-detected IP address;

c) Systems that cross-reference submitted data against existing data for other accounts, such as the use of the same credit card or device by several customers;
Systems that interface with third party data sources to import information that may assist in detecting incidence of fraud or money laundering across a number of payment service providers;

- On-chip controls that impose purse rules, such as those specifying the POS terminals or other cards with which the purse may transact;

- On-chip controls that impose purse limits such as transaction or turnover limits;

- On-chip controls that disable the card when a given pattern of activity is detected, requiring interaction with the issuer before it can be re-enabled;

- Controls that are designed to detect and forestall the use of the electronic money product for money laundering or terrorist financing in accordance with the typologies identified for such a product.

3.47. Information obtained through monitoring must be reviewed as part of the ongoing risk assessment; issuers must apply customer due diligence measures and monitoring appropriate to the risks.

3.48. Issuers are reminded that in the event that potentially suspicious activity is detected by internal systems or procedures, they must comply with their obligations under POCA and the Terrorism Act 2000 (see Part I, Chapter 6) to report possible money laundering or terrorist financing.

**Enhanced due diligence**

3.49. The Money Laundering Regulations 2017 require enhanced due diligence to be undertaken in all situations where the risk of money laundering is perceived to be high. These include instances where the customer is not physically present for identification purposes, as well as in respect of business relationships or occasional transactions with politically exposed persons (PEPs).

3.50. Where electronic money purses are purchased or accounts opened in a non-face-to-face environment, issuers must take specific and adequate measures to address the greater risk of money laundering or terrorist financing that is posed (see Part I, paras. 5.3.85 to 5.3. 91 on the mitigation of impersonation risk arising from non-face-to-face transactions). Issuers may adopt means of verification other than those outlined in Part I, provided that these are commensurate to the risk associated with the business relationship.

3.51. The requirement for issuers to have systems and processes to detect PEPs will be proportionate to the risk posed by the business relationship, as will the degree of enhanced due diligence required for PEPs. Issuers should focus their resources in a risk sensitive manner on products and transactions where the risk of money laundering is high. Further guidance on the application of the risk-based approach to PEPs is provided in Part I, paras. 5.5.24 to 5.5.28.

3.52. In all other high risk scenarios, issuers should have regard to the guidance in Part I Chapter 5.

**Multiple-card products**

---

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

9 If an electronic money purse meets the conditions for the e-money specific exemption, no PEP-related processes are required, even though the customer may be a PEP.
3.53. Issuers whose products enable two or more cards to be linked to a single account must establish whether they have entered into one or more business relationships, and must verify the identity of all customers with whom they have a business relationship.

3.54. Issuers should also consider whether the functionality of the second card may give rise to beneficial ownership.

3.55. Issuers should consider undertaking CDD even in the absence of a business relationship with, or beneficial ownership by, additional card holders on a risk-based approach. Where additional card holders remain non-verified, issuers must nevertheless implement controls effectively to mitigate the greater risk of money laundering and terrorist financing to which these products are exposed.

Verification of identity – merchants

3.56. The FCA expects electronic money issuers to understand who their merchants are in order to guard against the risk that their electronic money products might be used for money-laundering or terrorist financing.

3.57. Issuers must therefore apply ongoing due diligence to merchants on a risk-sensitive basis in accordance with Part I, Chapter 5. This includes the requirement to undertake adequate due diligence on the nature of the merchant’s business and to monitor the relationship.

3.58. In person-to-person systems, the boundary between consumers and merchants may be blurred; consumers may not register as merchants, but may nevertheless carry on quasi-merchant activity. In this case issuers:

- Should have systems in place that provide a means of detecting such activity.
- When such activity has been detected, apply due diligence measures appropriate to merchants.

3.59. Issuers may allow merchants to benefit from the €250 monthly turnover and €100 redemption allowance in order to enable the online recruitment of small merchants. This does not, however, alter the requirement to undertake adequate due diligence on the nature of the merchant’s business.

Wire Transfer Regulation

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

Scope

3.61. Issuers may be subject to the requirements of the WTR in their role as PSP of the payer, PSP of the payee or intermediary PSP.

3.62. Only those issuers that offer products that are used for person-to-person transfers or where the number of the e-money instrument does not accompany all transfers flowing from the transaction are subject to the requirements of the WTR.

3.63. Where an electronic money purse is funded through a card payment, this funding transaction is a payment for goods and services and is therefore out of scope according to Article 2(3) of the WTR (also see Part III, para. 1.17).

Verification requirements under the WTR
3.64. Verification of information under the WTR should be undertaken using a risk-based approach as provided for elsewhere in this guidance or as set out in Part III.

3.65. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payer by the PSP of the payer unless the funds are received in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.

3.66. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payee by the PSP of the payee unless the funds are paid out in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.

Redemption of electronic money

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

3.68. Where redemption is made in cash, this benefits from the exemption from the WTR for cash withdrawals from a customer’s own account under Article 2(4)(a).

Use of agents and distributors

3.69. Issuers may distribute or redeem electronic money through an electronic money distributor or can offer payment services through a payment services agent. Payment services agents must be registered with the FCA. Issuers are ultimately responsible for compliance with AML-related obligations where these are outsourced to their distributors and payment services agents. Issuers must be aware of the risk of non-compliance by their outsourced service providers and should take risk-based steps to monitoring the extent to which outsourced services are complying with their AML/CFT policies. Issuers must take measures to manage this risk effectively.

3.70. Issuers should apply the same customer due diligence measures to distributors as they do to merchants.

3.71. The FCA expects issuers to carry out fitness and propriety checks on payment services agents of electronic money issuers. These checks should include, among others, the assessment of the agents’ honesty, integrity and reputation in line with Chapter 3 of the FCA’s electronic money approach document.

3.72. Issuers are required to supply the FCA with a description of the internal control mechanisms their payment services agents have in place to comply with the Money Laundering Regulations 2017 and the Proceeds of Crime Act 2002. Where the payment services agent is established in another EEA jurisdiction, the issuer must ensure their AML systems and controls comply with local legislation and regulation that implements the 4th Money Laundering Directive. Issuers must also take reasonable measures to satisfy themselves that their payment services agents’ AML/CFT controls remain appropriate throughout the agency relationship.

Central contact points

3.73. Depending on their activities, when distributors or payment services agents are used to passport services to another EEA jurisdiction, these may be regarded as establishments in a form other than a branch and some member states may require issuers to establish a central contact point on their territory. The Joint Committee of the European Supervisory Authorities is developing
3.74. Regulation 22 of the Money Laundering Regulations 2017 gives supervisors the FCA the power to request payment service providers and electronic money issuers to appoint a person to act as a Central Contact Point in the UK if they are established in the UK in a form other than a branch and have their head office in an EEA state, a firm is based abroad on any issue relating to the prevention of money laundering or terrorist financing.

3.75. What amounts to an establishment is defined in the Treaty, and guidance on the meaning of establishment has been issued by the European Commission in 1997.10

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

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

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

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

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

The key drivers of risk

7.3 Part I, Chapter 4 states that any risk-based approach to AML needs to start with the identification and assessment of the risk that has to be managed and identifies key elements (or drivers) of risk as follows:

- products and services offered (including product features)
- party (e.g. the customer and any associated party such as the beneficial owner);
- jurisdictions operating in oversea connections;
- distribution channels (to deliver the products, services and transactions); and
- the complexity and volume of transactions and payment methods.

7.4 In addition to the risks identified above, the increasing volume of activities outsourced by insurers brings an additional dimension to the risks that the insurer faces, and this risk must be actively managed - see Part I (2.7 ff). Insurers that outsource activities should assess any possible AML/CTF risk associated with the outsourced functions, record the assessment and monitor the risk on an ongoing basis.

7.5 FCA regulated firms cannot contract out of their regulatory responsibilities, and they remain responsible for systems and controls in respect of the activities outsourced, whether within the UK or to another jurisdiction. In all instances of outsourcing, it is the delegating firm that bears the ultimate responsibility for the duties undertaken in its name. This includes ensuring, via relevant periodic reviews that the provider of the outsourced activities has satisfactory AML/CTF systems, controls and procedures.
7.6 Based on the views of insurance firms, the majority of this guidance focuses on risks from a product-led perspective; however, there are circumstances in which a customer’s profile, activity and complexity of transaction may add to the product risk. This is particularly the case with regard to Politically Exposed Persons – see Part I (5.5.1 ff). A firm must ensure that their own risk-based approach is appropriate to the particular circumstances they face — see Part I (4.2ff).

Politically Exposed Persons (PEP)

7.7 Part I (5.5.1 ff) sets out general provisions for identifying, establishing business with, and monitoring PEPs. This sectoral guidance sets out the fundamental risks and business practices that insurers may wish to consider when developing a risk-based procedure. These risks and business practices may change, and it is therefore important that insurers monitor these developments and adjust their procedures accordingly.

7.8 When developing a procedure for identifying PEPs, insurers should target those areas of business that are at the greatest risk of having customers who meet the PEP criteria.

7.9 Firms may consider using criteria such as accounts with non-UK residents and investment value to determine their risk-based approach to PEP identification and additional information can be found in the FCA PEP guidance.

7.10 It is expected that this risk-based procedure will make the volume checking of new customers unnecessary. However, adequate measures to check PEP status for those customers meeting the high risk criteria should be undertaken during the course of establishing the business relationship. If a PEP is identified at this stage, senior management approval is required for establishing a business relationship. In the case of identifying an existing customer as a PEP, senior management approval for continuing the business relationship must be obtained as soon as practicable upon identifying a PEP.

7.11 The identification of a customer as a PEP is not in itself cause for suspicion, and must not be used for reasons to reject or exit a business relationship, but requires an enhanced level of due diligence in line with the guidance set out in Part I. FCA-regulated firms should also have regard to the separate guidance on the treatment of PEPs published by the FCA in July 2017. In some cases enhanced due diligence may trigger suspicions that the client is attempting to store or launder the proceeds of crime, including corruption. In such cases, a SAR and consent request must be submitted to NCA, following the guidance set out in Part I, chapter 6.

Geographical Risk

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

Distribution Risk

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

---

11 For the purposes of this guidance, a non UK resident is a person defined as such for UK tax purposes.
will be non face-to-face sales, such as online, postal or telephone sales.

7.14 For business sold through agencies, such as financial advisers, agency acceptance and ongoing management procedures may already meet the requirements set out in Part I paragraphs 5.6.26 and 5.6.27. The MLRO should ensure that he is comfortable with the vetting processes undertaken by the firm’s distribution arm, for advisers, prior to the issue of and throughout the agency agreement. This should include the ability of the intermediary to provide copies of the underlying documents or data on request. The MLRO should be aware and satisfied with the level of monitoring of any material breaches/financial difficulties, which might call into question the agent’s status as fit and proper.

7.15 Once a business relationship is established with an intermediary, the Confirmation of Verification of Identity is the record for the purpose of meeting the record keeping requirements (this is irrespective of any outsourced administrative arrangement) and should be retained in accordance with the guidance provided in Part I, paragraphs 5.6.4ff. If, in the course of normal business, the intermediary’s standards are called into question, the insurer should review its status as a provider of CVIs. For higher risk business, such as non-UK, the MLRO will need to be satisfied that the level of customer due diligence carried out by the third party is commensurate with the risk and may wish to request copies of the underlying evidence obtained by the intermediary.

Product Risk

7.16 The remainder of this sectoral guidance concentrates on product risk. This is because, in the insurance sector, the nature of the product being sold is usually the primary driver of the risk assessment. This is because of the different nature of each category of products (protection, pensions and investments) and the fact that each product’s features are defined and potentially restricted; i.e., some will only pay out on a verifiable event such as death or illness, whilst others are accessible only after many years of contributions. As well as limiting the flexibility of these products as potential money laundering vehicles, the restrictions also enable firms to more readily profile the products for ‘standard’ (and conversely, ‘non standard’ or ‘suspicious’) use by customers.

7.17 A number of products sold by firms in the insurance sector, including General Investment Accounts (GIAs), single premium investment bonds and certain pensions, do feature increased flexibility/risk. This should be acknowledged in the application of the risk-based approach.

7.18 The following are features which may tend to increase the risk profile of a product:

- accept payments or receipts from third parties;
- accept very high value or unlimited value payments or large volumes of lower value payments;
- accept cash payments;
- accept frequent payments (outside of a normal regular premium policy);
- provide significant flexibility as to how investments are managed to be liquidated quickly (via surrender or partial withdrawal) and without prohibitive financial loss;
- be traded on a secondary market;
- be used as collateral for a loan and/or written in a discretionary or other increased risk trust;
- accept overpayments;
- provide access to funds;
- available on a Platform.

7.19 The following are features that may tend to reduce the risk profile of a product:
• restricted capacity to accept third party receipts or make third party payments;
• have total investment curtailed at a low value due to either the law or a firm’s policy;
• be relatively small value regular premium policies that can only be paid via direct debit;
• require the launderer to establish more than one relationship with a firm or another official body (e.g., certain types of pension products where the customer has to set up the product with the provider and to get HMRC approval and possibly appoint a Pensioner Trustee);
• have no investment value and only pay out against a certain event (death, illness etc) that can be checked by the product provider; and/or be linked to known legitimate employment.

7.20 The above are general lists of characteristics and are indicative only. Firms are strongly discouraged from using the lists in isolation for a mechanical ‘tick box’ style exercise. No characteristic acts of itself as a trigger. Not all products that may be used, say, as collateral for a loan, are automatically ‘increased risk’ by virtue of one characteristic alone. These general characteristics are given so that firms may weigh them up in overall balance for specific, branded products against their knowledge of the customer and their business.

7.21 Platform or ‘wrapper’ product offerings are those where a variety of products are offered to various target markets under an overarching ‘wrapper’ arrangement. These products may form, in effect, a portfolio arrangement for underlying clients or members, sold via arrangements conducted between the product provider and a third party - typically a regulated introducer (financial adviser), Employer or similar. They may encompass a variety of risk factors that drive the level of customer due diligence (see paragraphs 7.2 to 7.28).

7.22 Firms may wish to consider whether they should apply a standard level of customer due diligence to the whole ‘platform’ or ‘wrapper’, or whether to graduate the level of customer due diligence dependent on the actual product occurrence and specific risk factors as/when they arise. The customer due diligence should be conducted as appropriate, and before trading commences on the ‘platform’ or ‘wrapper’, in accordance with paragraphs 7.1 to 7.57 and financial sanctions guidance in Part III, Section 4. Whichever approach is used, a firm should ensure that it documents its approach and is satisfied that the approach adequately addresses the money laundering and terrorist financing risks according to the combination of risk factors inherent in the ‘platform’ or ‘wrapper’ arrangement.

7.23 Where apparent inconsistencies exist, firms are expected to exercise judgement accordingly. For example certain pension products and platform based portfolio arrangements accept contributions from employers. Third party payments are normally indicative of increased risk according to the list in 7.18, however for such products, there is some risk reduction in respect of source of funds. Some of the other features of pension products (the restricted access to funds up to the age of 55, and the involvement of HMRC), also reduce the product risk.

7.24 It is stressed that risk levels attributed to generic products in this document are intended to provide a starting point for a firm’s risk assessment. Firms should consider whether their own, branded versions of those generic products possess features (such as a facility for top up payments or prohibition from receiving/making third party payments) which raise or lower the risk level. Equally, taking account of other risk drivers which might be identified (for example, the geographical location of a customer) may lead a firm to ‘upgrade’ or downgrade the overall risk level of a product from that indicated in this guidance. Part I, section 5.5 discusses risk drivers that are not specific to insurance products. Also, where a proposition for business involving an intermediate or reduced risk product is exceptional due to the size, source of funds or for another reason that suggests risk of fraud, money laundering or other usage of proceeds of crime additional due diligence will be appropriate perhaps via existing anti-fraud or other business risk management procedures.
Three overall risk levels

7.25 Firms in the insurance sector have carried out risk profiling of their products, applying the risk assessment criteria detailed above. This guidance draws on that work and establishes three overall levels of risk for insurance products in an AML context. The risk level determines what work a firm needs to carry out to meet industry standards. The three levels are:

a) reduced risk;
b) intermediate risk; or
c) increased risk.

7.26 When attributing an appropriate risk level, it is important to keep insurance risk in its wider context. As already noted, the majority of insurance products do not deliver sufficient functionality and flexibility to be the first choice of vehicle for the money launderer.

7.27 The products identified as ‘increased risk’ are therefore categorised as such only in the context of the insurance sector and are not intended to equate to references to ‘high risk’ in the wider context of the financial services industry as a whole.

7.28 The risk level attributed should always be based on the underlying product, irrespective of how it is described in the product provider’s literature (i.e., substance prevails over form). Firms should expect to be in a position to justify the basis on which the risk assessment criteria have been applied.

7.29 Risk management is a continuous process (as noted in Part I, paragraph 4.64). The risk assessment process is not a one-time exercise, and it must be revisited and reviewed on a regular basis.

7.30 Finally, there is a need to monitor the environment in which the firm operates. It should be recognised that success in preventing money laundering in one area will tend to drive criminals to migrate to another area, business, or product stream. Firms should be aware of current risk assessments of money laundering/terrorist financing risk in the insurance sector and take them into consideration, along with trends they experience themselves. If displacement is happening, or if customer behaviour is changing, the firm should be considering what it should be doing differently to take account of these changes. A firm's anti-fraud measures will also help it understand its customers and mitigate the money laundering risks.

1 - Reduced risk level

7.31 Some groups of products, due to their inherent features, are extremely unlikely to be used for money laundering purposes. Some of these are recognised by the Money Laundering Regulations as potentially qualifying for Simplified Due Diligence [See Regulation 37(3)(b)]. Others, such as lifetime annuities are considered part of the pensions product. The table below shows these products in their respective categories of protection and pensions. The table also shows a number of the typical features (or restrictions) of each product, which serve to limit their potential as money laundering vehicles and so qualify them for this risk level.

7.32 Risk levels attributed to generic products in this section are intended for guidance only. Firms should consider whether their own branded versions of these generic products have features that either reduce or increase this indicative risk level.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Term life assurance</td>
<td><strong>Typical features:</strong> Timing of verification for pure</td>
</tr>
<tr>
<td>Protection Products (Part I: 5.2.3., ML Regs 37(3), Part II 7.31)</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Only pays out on death of assured</td>
<td></td>
</tr>
<tr>
<td>No surrender value</td>
<td></td>
</tr>
<tr>
<td>Small, regular premiums: additional payments by customer not possible</td>
<td></td>
</tr>
<tr>
<td>Large premiums will normally require medical evidence</td>
<td></td>
</tr>
<tr>
<td>No investment element</td>
<td></td>
</tr>
<tr>
<td>Once term of policy is finished no payout and policy ceases</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timing of verification for pure protection products (Part I: 5.2.3., ML Regs 37(3), Part II 7.31)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only pays out on medical evidence and proof required as to loss of income</td>
</tr>
<tr>
<td>No surrender value</td>
</tr>
<tr>
<td>Small, regular premiums: additional payments by customer not possible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timing of verification for pure protection products (Part I: 5.2.3., ML Regs 37(3), Part II 7.31)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only pays out on medical evidence</td>
</tr>
<tr>
<td>No surrender value</td>
</tr>
<tr>
<td>Small, regular premiums: additional payments by customer not possible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timing of verification for pure protection products (Part I: 5.2.3., ML Regs 37(3), Part II 7.31)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only pays on medical evidence</td>
</tr>
<tr>
<td>No surrender value</td>
</tr>
<tr>
<td>Premiums paid by employer – no member funding</td>
</tr>
<tr>
<td>Relatively small regular premiums</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timing of verification for pure protection products (Part I: 5.2.3., ML Regs 37(3), Part II 7.31)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long term savings vehicle - No surrender value</td>
</tr>
<tr>
<td>Product may not be used as collateral</td>
</tr>
</tbody>
</table>

### Pensions

5 Pension, superannuation or similar schemes which provide retirement benefits to employees (see footnote 8), where contributions are made by an employer or by way of deduction from an employee’s wages and the scheme rules do not permit the assignment of a member’s interest under the scheme (see footnote 9)
### 6 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 37(3) |

### 7 Rebate Only Personal Pension ("RPP")

| o Only funded by National Insurance Contribution rebates payable as a result of an individual being contracted out of SERPS or S2P |
| Qualifies for Simplified Due Diligence |

### 8 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 37(3) |

---

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

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

### Customer due diligence

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

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

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

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

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

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

Note - HMRC does not now issue approval letters. However, if the firm has any concerns, on application and with the relevant authority, HMRC will provide documentary confirmation regarding the existence of the scheme.
b. Verifying the identity of the employer, or other corporate entity paying into the fund, in accordance with Part I, Chapter 5. Check that the firm is trading and appropriate to provide employees with a pension through a Companies House search. Persons with Significant Control register (PSC) check or a visit to premises. Beneficial owners should be identified e.g. on the Companies House search or checking the PSC register, however it is not necessary to verify their identities. Ongoing monitoring, however, is still required.

7.36 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a Bankers Draft or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.

7.37 In addition, the destination of funds at the time of redemption can be used as evidence of identity in cases where there has not previously been a requirement to verify, for example where the firm had been able to rely on an exemption.

7.38 In these cases, depending on the firm’s assessment of the risk presented by the situation, including the circumstances in which the customer acquired the investment, it may be possible to satisfy the standard identification requirement by means of a payment to an account with a UK or EU regulated credit institution in the sole or joint name of the customer. The old style Financial Adviser Certificates (confirmations of identity) had a tick box “Existing Customer Pre April 1994” – this exemption is not transferable to Insurers. The firm may, however, have completed a current customer review exercise to pick the verification of these customers up.

Monitoring

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

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

II - Intermediate risk level

7.41 The intermediate risk level has been attributed to a group of products whose inherent features pose some risk of use for the purposes of money laundering or terrorist financing but they are significantly less than the risks posed by the “increased risk” grouping of insurance products. Some risk is acknowledged in the case, for example, of products with a facility for ‘top up’ payments, and therefore the standard level of due diligence is appropriate. The table below shows these products in their respective categories of protection, savings and pensions, together with some of their typical features or restrictions.

7.42 Risk levels attributed to generic products in this section are intended for guidance only. Firms should consider whether their own branded versions of these generic products have features that either reduce or increase this indicative risk level.
### Whole of Life

**Typical features:**
- may accrue some surrender value
- benefits usually payable on death or diagnosis of terminal illness
- or, in some cases, critical illness of the policyholder
- partial surrenders are normally allowed within specified limits
- qualifying whole of life plans will comply with the rules applicable to qualifying life policies

### Savings and Investments

#### Life assurance savings plan

**Typical features:**
- Long term savings plan often for retirement
- Requires at least 5 years to gain positive return on investment
- Often unable to be surrendered in first or second year, with penalties in years three to five
- Additional 'top up' payments may be permitted
- Sum assured/premium relationship broadly complying with HMRC Qualifying Rules

#### Endowments

- Long term savings plan for a set term, were often linked to mortgages
- Sum assured/premium relationship broadly complying with HMRC Qualifying Rules
- Usually long term, 10-25 years

#### Trustee Investment Plan ("TIP")

- The plans are governed by trustees
- The plans must be associated with a pension scheme
- All cash flows into and out of the Plan must be via the trustees
- Not FCA-regulated

### Pensions

#### Group Personal Pension ("GPP")

**Typical features:**
- Long term policy, usually up to 40 years
- No access to funds in normal circumstances until the policyholder reaches 55 years of age
- Employee and employer contributions

#### Group Stakeholder Plan

- Long term policy, usually up to 40 years
- Portable pension pot
- HMRC registered scheme
- Annual and lifetime limits apply
- No access to funds in normal circumstances until the policyholder reaches 55 years of age

#### Income Drawdown Flexible Pension Plan Phased Retirement Plan

- Typical features:
  - Policies only open to individuals between the ages 55 – 75, and people who have already accrued by a pension fund

#### Free Standing Additional Voluntary Contribution Plan ("FSAVC")

- Contributions cap set by pensions legislation and monitored by scheme administrator
- Transfers are only possible to another regulated
| 9 Stakeholder Plan | o Long term policy, usually up to 40 years  
|                    | o No access to funds in normal circumstances until the policyholder reaches 55 years of age  
|                    | o HMRC registered scheme  
|                    | o Annual and lifetime limits apply |
| 10 Personal Pension Plan (not SIPP or SSAS) | o Long term policy, usually up to 40 years  
|                                            | o No access to funds in normal circumstances until the policyholder reaches 55 years of age  
|                                            | o HMRC registered scheme. Transfers are possible, but only to another registered scheme.  
|                                            | o Annual and lifetime limits apply |
| 11 Self Invested Personal Pension ("SIPP") | o Provides a choice of allowable investments, including commercial property, i.e., can be used to buy business premises.  
|                                            | o Long term policy, usually up to 40 years  
|                                            | o No access to funds in normal circumstances until the policyholder reaches 55 years of age  
|                                            | o HMRC registered scheme. Transfers are possible, but only to another registered scheme.  
|                                            | o Annual and lifetime limits apply |
| 12 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  
|                                            | 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.  
|                                            | o Not FCA-regulated |
| 13 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 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, me  
|                                            | o Not FCA-regulated |
| 14 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 55 and 75.  
|                                            | o Normally the end product of a pension transfer  
|                                            | o Annuity usually purchased with one one-off payment to provide income for life. |
Purchased Life Annuity ("PLA") Hancock Annuity

- No return of cash lump sum at end of the term selected or when customer dies
- Once annuity purchased, purchaser cannot alter the arrangements or cash it in.

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

Customer due diligence

7.44 The recommended industry standard for intermediate risk products is as follows: Verify the identity of the customer and/or the relevant parties, as per the guidance set out in Part I, Chapter 5, at the outset of the business relationship.

7.45 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a Bankers Draft or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.

7.46 In accordance with Part I, companies must identify the beneficial owner, following the guidance in Part I, paragraphs 5.3.8 to 5.3.13.

7.47 In addition, the destination of funds at the time of redemption can be used as evidence of identity in cases where there has not previously been a requirement to verify, for example where the firm had been able to rely on an exemption. In these cases, depending on the firm's assessment of the risk presented by the situation, including the circumstances in which the customer acquired the investment, it may be possible to satisfy the standard identification requirement by means of a payment to an account with a UK or EU regulated credit institution in the sole or joint name of the customer. The old style Financial Adviser Certificates (confirmations of identity) had a tick box “Existing Customer Pre April 1994” – this exemption is not transferable to Insurers. The firm may however have completed a current customer review exercise to pick the verification of these customers up.

Monitoring

7.48 Insurance companies should have a programme of monitoring which reflects the intermediate risk status of the products mentioned above. A firm should ensure its employees are adequately trained to identify and report unusual business activity to the firm’s nominated officer. Enhanced monitoring may be considered for those pension holders over the age of 55 years of age to reflect the increased pensions freedoms brought in by the government in 2014. This is reflective of the increased access for these individuals to drawdown and payback into pension pots.

7.49 Firms should undertake ongoing monitoring for patterns of unusual or suspicious activity to ensure that higher-risk activity can be scrutinised. For example, top-up payments when these are much larger than current holdings, or for EPPs & SSASs, are areas that should receive scrutiny, as well as loans taken out using product as collateral.

Frequently asked questions in relation to intermediate risk – please see Annex 7-1
III Increased risk level

7.51 The increased risk level has been attributed to a product whose inherent features open the possibility to their being used for money laundering purposes. The product may have a facility for third party and/or ‘top up’ payments, or is perhaps negotiable, and therefore an enhanced level of due diligence by asking for more information is appropriate. It is to this risk level that the majority of a firm’s AML resource will normally be directed. The table below shows the product together with the features.

7.52 Risk levels attributed to the generic product in this section are intended for guidance only. Firms should consider whether their own branded versions of this generic product have features that either reduce or increase this indicative risk level. As stated before, the increased designation is used here to reflect the different average levels of investments in pensions, savings and other investment products experienced by firms and intermediaries across the sector.

<table>
<thead>
<tr>
<th>Protection</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Savings and investments</td>
<td>Typical features:</td>
</tr>
<tr>
<td>1 Single premium investment bonds, including:</td>
<td>o Open ended investment</td>
</tr>
<tr>
<td>• With profits</td>
<td>o Additional ‘top up’ payments permitted by policy holder and by third parties</td>
</tr>
<tr>
<td>• Guaranteed</td>
<td>o May be segmented and individual segments may be assignable</td>
</tr>
<tr>
<td>• Income</td>
<td></td>
</tr>
<tr>
<td>• Investment</td>
<td></td>
</tr>
<tr>
<td>• Offshore international bonds</td>
<td></td>
</tr>
<tr>
<td>Pensions</td>
<td>None</td>
</tr>
</tbody>
</table>

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

Customer due diligence

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

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

AND

2. Acquire prescribed information at the outset of the business relationship to satisfy the additional information requirements of Part I, Chapter 5:
   a. source of funds for the transaction (e.g., a UK bank account in own name);
   b. employment and salary details; and
   c. source of wealth (e.g., inheritance, divorce settlement, property sale)
3. If the firm determines that the risk of the business is increased further by the customer and/or payment and/or location (e.g. the customer is a PEP in a high risk country), the firm should consider, as part of its EDD, whether the information regarding source of wealth should be evidenced. For example, for source of wealth from inheritance, a copy of the Will could be requested.

7.55 Firms are not required to assume that a payment from an unidentified source (e.g., by wire transfer from a UK bank or building society or a UK Building Society counter cheque that does not identify the account from which it is made) is being made by a third party unless they are aware of some fact that suggests that this is, or may be the case.

7.56 An insurer must, where appropriate, verify the identity of the beneficial owner for increased risk products in line with the provisions in Part I, paragraphs 5.3.8 to 5.3.13.

Monitoring

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

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

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

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

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

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

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

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

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

a) For reduced risk level products, firms may accept personal cheques and other payment instruments drawn on a customer’s account as satisfying the requirement to verify the customer’s identity.

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

(v) What about verification on reduced risk level pension transfers?
There is no requirement to verify identity if both of the following conditions are satisfied:

1. the transfer is from an Occupational Pension Scheme which is not a Executive Pension Plan (“EPP”) or a Small Self Administered Scheme (“SSAS”); and

2. the transfer is to an Occupational Pension Scheme (which is not an EPP or a SSAS) or is to a S32 buy out plan with no additional funding.

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

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

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

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

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

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

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

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

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

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

Due to restrictions on releasing funds, pensions and annuities are in the reduced and intermediate risk categories; however, with the rise in pension liberation, there are increasing opportunities to obtain funds from these products.
Firms may also develop new, innovative products, to provide an income in retirement, given that an annuity will no longer be a compulsory option, as it has been for many pension plan maturities.

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

Intermediate risk

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

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

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

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

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

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

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

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

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

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

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

If a member requests that their Tax Free Cash amount is paid to a third party, additional checks will be required, including verification of the third party.
Contributions from any third party not connected to the pension scheme will require the third party’s identity to be verified in accordance with Part I, chapter 5.

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

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

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

Trustees

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

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

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

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

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

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

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

(vii) What about traded endowments?

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

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

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

Subject(s) of such an order that are explicitly nominated to receive funds should be regarded as the beneficial owner(s), and their identity may also be verified by reference to the court
(x) **What if a payment on death is to be made direct to a beneficiary?**

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

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

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

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

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

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

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

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

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

In all cases, regardless of risk, if payment is made direct to a beneficiary at the request of a trustee, the identity of the beneficiary should be verified, PEP and sanction checked prior to payment being made, if this has not already been done. Where payment is being made to the trustee(s), the trustee(s) should be verified, PEP and sanction check if this has not already been done.
* It is recommended that firms liaise with their legal consultants over whether or not to request a copy of the trust deed.

Increased Risk

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

The relevant parties are summarised in the table below:

<table>
<thead>
<tr>
<th>Savings/investments</th>
<th>Relevant parties to be identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Bonds</td>
<td>o Policy holder or applicant</td>
</tr>
<tr>
<td></td>
<td>o All payers if different to policy holder</td>
</tr>
<tr>
<td></td>
<td>o All payees if different to policy holder</td>
</tr>
<tr>
<td></td>
<td>o Beneficial Owners (verification on higher risk cases – see FAQ v below)</td>
</tr>
<tr>
<td>Pensions</td>
<td>None</td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>Savings/investments</th>
<th>Suggested practice for monitoring and control</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Bonds</td>
<td>o Cancellation (i.e., applications not proceeded with after funds received)</td>
</tr>
<tr>
<td></td>
<td>o Early surrenders (i.e., within a certain time period, which is to be specified by individual firms) over a certain € threshold</td>
</tr>
<tr>
<td></td>
<td>o Multiple partial surrenders, totalling up to (say) 75% of original investment, within the specified time period</td>
</tr>
<tr>
<td></td>
<td>o Top up payments over a certain € threshold (dependent on individual firms’ assessment of materiality) and frequency</td>
</tr>
<tr>
<td></td>
<td>o Third party payments of any value o Non UK residents</td>
</tr>
<tr>
<td>Pensions</td>
<td>None</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

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

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

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

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

Where any party requiring verification is represented by an individual or firm appointed under a Power of Attorney, the identity of the Attorney should also be verified using the principles established in Part I, paragraphs 5.3.99-5.3.101.
What about cancellation during the “cooling-off period” leading to a refund of premium paid? In some cases, the customer has not yet been verified by that time.

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

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

What if a payment on death is to be made direct to a beneficiary?

Should executors or administrators instruct payments to be made directly to the beneficiaries, the identity of the beneficiaries should be verified, if not already done so, in line with the guidance in Part I, paragraphs 5.3.8 to 5.3.13, prior to the payment being made. Sanction and PEP checks should also be undertaken.
7A: General insurers

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

Introduction

7A.1 The intention of this guidance is to provide clarification for General Insurers as to their obligation to report suspicious activity under the Proceeds of Crime Act 2002 (POCA), comply with sanctions legislation and explain the new powers granted to H.M. Treasury under the Counter Terrorism Act 2008. General Insurers are not within the regulated sector, as defined under the Money Laundering Regulations 2017, but in certain circumstances they are required to report suspicious activity to the National Crime Agency (NCA).

7A.2 Part 7 of POCA came into force on 24 February 2003. This sectoral guidance focuses on the obligations of general insurers and is designed to assist General Insurers in applying legislation consistently. The objective is to help general insurers refine their current practices and to identify whether they are complying with POCA.

7A.3 This guidance is not a replacement for detailed advice on specific activities and problems and it should not be regarded as a substitute for legal advice on any of the topics discussed. General insurers should, periodically, seek their own legal advice to ensure that their understanding of the legal framework is up to date.

Proceeds of Crime Act and the Terrorism Act

7A.4 The offences under POCA and the Terrorism Act relate to any activity involving criminal or terrorist property (including, sometimes, the criminal or terrorist act itself). This is a much broader definition than the commonly understood definition of money laundering (i.e., the movement, layering and concealment of criminal funds). A company, for example, can commit an offence under POCA by unwittingly facilitating an act of fraud.

7A.5 Obligations under POCA and the Terrorism Act, in practical terms, vary depending on which sector is seeking to apply them. General insurance is considered to be a low risk sector for both money laundering and the concealment or conversion of the proceeds of crime. General insurance is regarded as being at greater risk from fraudulent claims, rather than as a conduit for the proceeds of crime or money laundering. The majority of general insurance products do not, per se, offer obvious scope to be of use to money launderers. There is, however, scope for insurers to become unwittingly involved in criminal offences such as fraudulent claims or deliberately providing inaccurate information at inception, which may trigger provisions under POCA for suspicion reporting.

Risk-based approach

7A.6 The guidance on money laundering prevention in Part I, addressed to the wider financial sector is risk-based. It is recommended that general insurers also adopt a risk-based approach to their obligations under POCA and the Terrorism Act 2000.

7A.7 The implementation of risk management can be a simple process depending on the range of products on offer and should be linked to the profile of the customer. Insurers who also offer life products will already be aware of the requirement to carry out Customer Due Diligence (CDD). A general insurer is not required to seek the equivalent level of information on their customers, but it
is recommended that risk management be considered by non-life insurers at the earliest possible stage e.g., when a potential customer makes an approach or when a broker advises the insurer of a new customer, as well as when policies are renewed or claims are submitted, based on the information an insurer has. It requires the full commitment and support of senior management and the active co-operation across business units.

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

7A.9 General insurers should consider the following:

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

Reporting Suspicious Activity

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

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

7A.12 During the claims process there may be suspicion on the part of a member of the claims team that the customer may be embellishing their claim and there may be a number of challenges and procedures that will be followed until the claim is agreed or declined. Whilst this process is ongoing the customer may be attempting to commit a fraud, but this is not a reportable offence under POCA.
7A.13 However, if a claim has been accepted and agreed and the insurer has paid the claim and subsequently it is discovered that there are reasonable grounds to know or suspect that the claim was false, then the reporting provisions under POCA are met and the insurer must file a suspicious activity report (SAR) with the NCA as soon as practicable. This is because any payment made as a result of the claim is now classified as criminal property and must be reported to the NCA.

7A.14 General insurers do not have an obligation to appoint a nominated officer to deal with disclosures of SARs. However, POCA applies to both regulated and unregulated sectors and SARs can be made to the NCA by any industry representative. If insurance firms elect to appoint a single point of contact who would be regarded as a nominated officer, there are additional obligations in respect of reporting to the NCA and where consent may be required, after an internal report is made to him/her. In practice, this means an obligation to submit a SAR (see Part I, Chapter 6). Failure to do so may mean he/she will commit an offence under section 332 of POCA. From a practical perspective it is advisable for someone to coordinate a company’s anti-money laundering procedures as well as administer obligations under POCA. This would give staff a contact that they can approach if they have any suspicions.

7A.15 If there is no nominated officer, employees should make disclosures to the NCA by way of a SAR. SARs can be submitted electronically or by post though the NCA is actively encouraging the use of the SAR Online system which can be found at www.nca.gov.uk.

Financial Sanctions

7A.17 Under the financial sanctions regime it is a criminal offence to make either funds or financial services available to the targets on the Financial Sanctions Consolidated List which are published and maintained by the Office of Financial Sanctions Implementation (OFSI). Financial sanctions apply to all companies, irrespective of whether or not they are regulated. The guidance contained in Part I, paragraphs 5.3.54-65, and Part III should be followed.

7A.18 Financial sanctions apply to all forms of payment and services offered. In respect of General Insurers this applies not only to the contract of insurance but could also apply to third party payments and providing replacement vehicles and articles. In relation to proliferation financing, the provision of insurance cover to shipments of goods which contravene related export controls could cause the insurer (or broker) to breach relevant legal and/or regulatory obligations. See Part II, sector 15: Trade finance, especially paragraph 15.28 and Annex 15-IV.

Counter Terrorism Act 2008

7A.20 The Counter Terrorism Act was enacted on the 26th November 2008 and introduces additional obligations on firms in the fight against money laundering, terrorist financing and the proliferation of nuclear, radiological, biological or chemical weapons. Directions under this act can only be given by HM Treasury.

7A.21 There are four specific instances where this Act may be used but only two of the directions may be given to General Insurers. These are the directions in respect of systematic reporting, where a direction may require a firm to provide such information and documents as may be specified in the direction relating to transactions and relationships with designated persons. The direction will specify to whom the information and documents are to be provided and the period within or the intervals at which they are to be provided.
7A.22 The second direction relates to **limiting or ceasing business.** Such a direction may require a firm not to enter into or continue to participate in a specified transaction or specified description of transactions or business relationships with a designated person or any transaction or business relationship with a designated person.

7A.23 Part I, section 5.8 provides further guidance on meeting obligations imposed under these directions.
9: Discretionary and advisory investment management

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

**Overview of the Sector**

9.1 *Investment management* includes both discretionary and advisory management of segregated portfolios of assets (securities, derivatives, cash, property etc.) for the firm's customers. Where investment management is provided as part of a broader "wealth management" service, readers should refer instead to Sector 5: *Wealth Management*.

9.2 Discretionary managers are given powers to decide upon stock selection and to undertake transactions within the portfolio as necessary, according to an investment mandate agreed between the firm and the customer.

9.3 Advisory relationships differ, in that, having determined the appropriate stock selection, the manager has no power to deal without the customer’s authority - in some cases the customer will execute their own transactions in light of the manager's advice. This should not be confused with "financial advice", which involves advising customers on their investment needs (typically for long-term savings and pension provision) and selecting the appropriate products. Financial advice is dealt with in Sector 6: *Financial advisers*.

9.4 The activities referred to above may be carried out for private or institutional investors. Note that guidance on the operation of investment funds, including those that are solely for institutional investors, is given in Sector 8: *Non-life providers of investment fund products*.

**What are the money laundering risks relating to investment management?**

9.5 In terms of money laundering risk, there is little difference between discretionary and advisory investment management. In both cases, the firm may itself physically handle incoming or outgoing funds, or it may be done entirely by the customer's custodian.

9.6 In either case, the typical firm deals with low volumes of high value customers, for which there should be a take-on process that involves a level of understanding of the customer's circumstances, needs and priorities and anticipated inflows and outflows of funds, in order to determine suitable investment parameters.

9.7 Firms should maintain ongoing contact, often face-to-face, with the customer in order to review market developments and performance, and review the customer’s circumstances, etc. Unexpected inflows/outflows of funds are not common occurrences - ad hoc requirements and movements are usually the subject of discussion between the firm and the customer.
9.8 In most cases, all money and other assets within the portfolio are held under the control of a regulated custodian, with money paid to or from the customer through their bank or building society account. Investment management is not a mechanism for the movement of assets from one person to another, although some third party payments may be made (e.g. in the case of private customers, for the payment of school fees).

9.9 The risk of money laundering to the investment management sector, in the context of the "typical" circumstances described above, would be low. Clearly, however, the risk will increase when dealing with certain types of customer, such as:

- offshore trusts/companies,
- higher-risk PEPs and
customers from higher risk countries,
other service features that a firm offers to its customers.

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

**Risk Based Approach**

9.10 As outlined in Part I Chapter 4, all firms must develop a risk based approach to mitigating the risk of their products and services being used for the purposes of money laundering or terrorist financing. Firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms should have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk.

9.11 Firms should assess the risk of the products they provide, the services they offer and the relationships that they have with their customer. Where a low degree of risk is determined then Simplified Due Diligence (SDD) may be applied. Where a high risk is identified then Enhanced Due Diligence (EDD) measures should be applied; in other circumstances, standard Customer Due Diligence (CDD) will apply.

**Product/Service Characteristics**

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

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Inherent risk</th>
<th>Industry Standard</th>
<th>Risk Mitigation</th>
<th>Risk Rating after mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex ownership structures, which can make it easier to conceal underlying beneficiaries</td>
<td>Medium</td>
<td></td>
<td>CDD is performed on the client and any beneficial owners, where required.</td>
<td>Low</td>
</tr>
<tr>
<td>Customers represented by a third party</td>
<td>Medium</td>
<td></td>
<td>Evidence of official appointment obtained.</td>
<td>Low</td>
</tr>
<tr>
<td>Involvement of an individual in a public position (PEP/RCA)</td>
<td>High</td>
<td></td>
<td>Screening of public source information (e.g. Worldcheck, Dow Jones). Enhanced CDD performed</td>
<td>High</td>
</tr>
</tbody>
</table>

### Transactions

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Industry Standard</th>
<th>Risk Mitigation</th>
<th>Risk Rating after mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction activity is high in value</td>
<td></td>
<td>Transaction inflows and outflows will be discussed with and notified to the appointed client manager in advance.</td>
<td>Low</td>
</tr>
<tr>
<td>Transaction activity is high in volume</td>
<td></td>
<td>Monitoring will identify any unusual trading patterns.</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Delivery Channels

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Industry Standard</th>
<th>Risk Mitigation</th>
<th>Risk Rating after mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to transact face-to-face</td>
<td></td>
<td>Regular contact between the client manager and the client will largely be on a regular basis.</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Geography

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

### Who is the customer for AML purposes?

9.12 The typical investors to whom investment managers provide services are high net worth individuals, trusts, companies, government bodies and other investing institutions such as pension schemes, charities and open/closed-ended pooled investment vehicles. In such cases, the firm’s customer will be the individual or entity concerned. The firm must also consider whether there are any beneficial owners or controllers.

9.13 Firms may also be contracted to provide investment management services to other appropriately regulated UK and overseas firms in respect of their own investments (e.g. life companies) or assets they are managing for others - in either instance the investment manager’s customer will be the other regulated firm, in which case the firm...
should determine the need to consider any underlying beneficial ownership or control on a risk based approach.

Customer due diligence

Verification of identity

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

Private individuals

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

Customers other than private individuals

9.16 When dealing with other types of customer, firms would normally be able to rely on the standard verification measures, including simplified due diligence for qualifying customers, as described in Part I, paragraphs 5.3.106 – 5.3.272.

9.17 For overseas pension schemes and charities, additional verification steps may be required, depending upon the risk associated with the type of customer and their location (e.g. in a higher risk jurisdiction).

9.18 For most charities, the firm will be able to regard those that may benefit from the charity as a class of beneficiary. As such, they do not need to be identified and verified individually. The members of occupational pensions schemes that do not qualify for simplified due diligence may be treated similarly.

9.19 In instances where the identities of beneficial owners or controllers must be verified individually, this may be done in accordance with Part I, paragraphs 5.3.8 – 5.3.13. If the circumstances of the relationship indicate that it is low risk (by virtue of the services to be provided or the specific nature of the customer), the identity of beneficial owners and controllers may be confirmed by the customer itself (see Part I, paragraphs 5.3.11 and 5.3.12). If CDD or EDD is to be applied then independent verification should be sought.

Mandates relating to third party investment vehicles
9.20 Some investment managers provide services to third party investment vehicles (e.g. hedge funds), which may be open or closed ended. Those firms must consider whether or not there is a need for them to look at the underlying investors in such vehicles. This will depend on the status of the vehicle and how it is operated in terms of dealing in its units/shares:

☐ Where such dealings are handled by an appropriately regulated entity (e.g. fund manager or transfer agent) or are traded on a regulated market or exchange, the investment manager does not need to be concerned with the underlying investors.

☐ If a vehicle operates under less stringent conditions than those described above, the firm may take a risk-based approach and ensure that it is satisfied, on an ongoing basis, with the checks that are carried out by whoever controls entry to the vehicle’s register of holders, and the information that will be available to the firm if required. Otherwise the firm will need to undertake its own risk-based customer due diligence, as necessary.

9.21 In any event, the firm must carry out appropriate due diligence on third party investment vehicles to establish and verify their form, status, purpose, and the identity of any persons who are in positions of control.

9.22 In most cases, the investors in such funds would be regarded as a class of beneficiary and so would not need to be verified individually. However, where the vehicle is being operated for “private” use by a specific group of individuals, verification of their identities as beneficial owners/controllers should be undertaken in accordance with the guidance given in Part I, paragraphs 5.3.8 - 5.3.13.

9.23 Investment management firms which provide services to unregulated vehicles such as hedge funds will find it helpful also to refer to Sector 20: Brokerage services to funds.

Custody and third party payments/transfers

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

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

9.25 Where the customer enters into an agreement directly with a custodian other than the firm, it is the custodian that should be concerned about third party payments and transfers. The firm should consider the issue itself, however, where it is involved in
the transmission of funds or otherwise passes instructions to the custodian regarding a receipt or withdrawal of funds/investments.

9.26 The firm may provide custody notionally as part of its service to the customer, but outsource the safe-keeping function to a sub-custodian. In these circumstances, the firm will usually instruct the sub-custodian regarding receipts or withdrawals from the portfolio and should therefore take appropriate steps to verify the identity of any third party that may be involved. The firm should also ensure that the issue is addressed, either by itself or by the sub-custodian, where the customer is able to instruct the sub-custodian directly.

9.27 The firm may perform the custody function in-house, in which case it must take appropriate steps itself to verify the identity any third parties that may be involved.

9.28 In any event, where the firm is asked to receive, make or arrange payment to/from someone other than a person it has verified as a customer or beneficial owner, it should seek to understand the reasons behind the payment and the capacity of the third party and consider the extent to which the identity of that third party may need to be verified.

Timing

9.29 Firms must verify a customer's identity as soon as practicable after first contact with the customer. While most institutional customers will be identified before funding their account, they are not prevented from entering into the relationship. Firms should take all reasonable steps to verify the customer's identity within a reasonable time. Where the firm is unable to verify the identity of the investor within a reasonable time it must, at that point, consider if the circumstances give any grounds to suspect money laundering or terrorist financing and act accordingly (see Part I, paragraph 5.2.8).

9.30 If, however, after such reasonable time, the firm has no grounds to suspect and is satisfied that the risk of money laundering is minimal, subject to its terms of business it must terminate the relationship and return any monies received to their source. Alternatively, if the firm is suspicious, it must submit a SAR to the NCA. If it does not receive consent to money laundering to return the money, the firm must freeze any funds or assets pending eventual verification (see Part I, paragraph 5.2.9).

9.31 From the point at which the firm concludes it should freeze an investment:

(a) it must not accept further investments from the customer until they provide the evidence of identity required by the firm;

(b) it may permit the investor to withdraw their investment upon production of the evidence of identity required by the firm;

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

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

Additional customer information

9.33 The client take-on process for investment management customers usually involves gaining an understanding of the customer, including their source of wealth and income, and their needs, and establishing at the outset the likely inflows and outflows of funds are likely. Developments in this area and updates to customer information should be sought periodically from the customer or his adviser.

9.34 The customer information, obtained for the purposes of agreeing the firm's mandate and the ongoing management of the customer’s portfolio, will usually comprise the additional information necessary to understand the nature and purpose of the relationship in a money laundering context, against which the customer's future activity should be considered.

Monitoring

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

Non-liquid transactions (including Real estate)

9.36 Some portfolios will include direct holdings in real estate. Unlike securities, the counterparties involved in the purchase and sale of direct holdings may not be other regulated financial institutions. Those purchases and sales will often involve special purpose vehicles, and in some cases will be owned via trusts and a wide variety of structures in a wide variety of jurisdictions which by their nature may increase the risk of coming into contact with the proceeds of crime.

9.37 Some portfolios will make direct investments in construction and development projects. The nature of these projects, and especially the risks of fraud, bribery and corruption and tax evasion may also increase the likelihood of coming into contact with the proceeds of crime.

9.38 The counterparty would not normally be regarded as a customer of the investment firm and consequently the firm would not be obliged to verify the identity of the counterparty itself. However, in order to mitigate what could be significant reputational risk, firms may wish to seek appropriate assurances from their own solicitors that the identity of the counterparty will have been verified.
9.39 These transactions are generally conducted through solicitors, and the counterparty's solicitor may agree to verify its customer’s identity. However, where they do not consent, firms must consider what level of information they require, this could, for instance, be in line with the firm’s risk based approach and with Chapter 5 of Part I.
11. Motor finance

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

Overview of the sector

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

Purchase agreements

11.2 Conditional sale is a contract between the finance company and the customer where the customer agrees to buy specific goods. It is normally a fixed cost, fixed term credit and the customer in practice exercises all the rights of the owner of the goods. However, in law, the ownership of the asset will not pass until certain conditions are met (normally that all payments under the contract have been made, but individual contracts may include other conditions).

11.3 Hire Purchase (HP) and Lease Purchase (LP). These are both agreements under which the customer will hire the vehicle for a fixed period of time. During this period the motor finance company will recover, through the instalments paid, the cost of the vehicle together with its charges. Once the agreement is paid in full, the customer has the option to purchase the vehicle for a nominal sum. Generally, the difference between the two agreements is that on HP the amount to be repaid is spread evenly throughout the agreement, whereas on LP a substantial sum is deferred to the final instalment.

11.4 Personal Contract Purchase (PCP) is in essence a purchase agreement (the definition would, therefore, be the same as HP and LP) with a Guaranteed Minimum Future Value (GMFV) placed on the goods by the finance company. The customer has the choice at the end of the agreement of either paying the GMFV and obtaining title to the vehicle or returning the vehicle (and not having to pay the GMFV).

11.5 Personal Loan is an agreement where the title passes immediately to the customer and an unsecured loan is provided to cover all or a proportion of the sale price.

Lease agreements

11.6 These are agreements where the customer leases the vehicle for a fixed period of time, but does not have the ability to obtain title. The motor finance company will reclaim the VAT on the vehicle and claim writing down allowances for tax purposes, as owner of the asset. A business customer can, dependent upon its tax position, claim both tax relief and proportion of the VAT on rentals paid. There are two types of lease:

A Finance Lease, where the customer takes the risk in the final value of the vehicle.
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\textsuperscript{12} are outside the scope of the ML Regulations\textsuperscript{13}. 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.

\textsuperscript{12} 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.

\textsuperscript{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.
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.

Who is the customer for AML purposes?

11.16 A customer may be a private individual or a business e.g., partnerships, companies, associations etc.

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

Customer due diligence

11.18 In a move to reduce fraudulent credit applications, members of the Finance & Leasing Association (FLA) have subscribed to an industry standard which sets out acceptable identification and verification checks across common sales channels for obtaining motor finance. The Industry Standard is set out in the attached Annex 11-I.

11.19 Compliance with the Industry Standard on proof of identity goes beyond the current money laundering requirements under simplified due diligence (SDD), which is directly relevant for low risk products such as hire purchase and leasing agreements. However, this Industry Standard should still be used in order to guard against fraud. On-going monitoring of the business relationship is still required under simplified due diligence (SDD).
INTRODUCTION

1. Finance and Leasing Association (FLA) motor finance members have both a legal and moral obligation to ensure that they correctly identify their customers in the credit application process in order to prevent financial crime and terrorist financing.

2. The requirements set out in the Money Laundering Regulations and the Joint Money Laundering Steering Group (JMLSG) Guidance are the minimum legal requirements that all FLA motor finance members must comply with in the battle against money laundering, fraud and terrorist funding. This document in no way seeks to replace members’ legal obligations.

3. The remainder of this Standard sets out the approach required by full FLA members to due diligence when considering a credit application and acceptable methods for conducting these checks. Appendix 1 outlines common sales channels available for obtaining motor finance and identifies for each what evidence of identification (Know Your Customer) and verification of this evidence (Prove Your Customer) is required to meet the Standard.

RISK ASSESSMENT

4. Members will undertake appropriate steps to identify, assess and mitigate the risks of money laundering and terrorist financing to which its business is subject, taking into account information made available by the FCA on risk factors that relate to their customers, products, services, transactions and delivery channels.

5. The assessment of the risks inherent to a member’s business will inform its risk-based approach which determines the level of due diligence undertaken for each individual customer. Risk assessments must be documented, kept up to date and made available to the FCA on request.

CUSTOMER DUE DILIGENCE (CDD)

6. There is a fundamental requirement to identify customers and verify their identity through CDD where they are individuals. Where the customer is a business, members should additionally identify its beneficial owners and be satisfied they know who the owners are. A beneficial owner of a business is a person who owns or controls more than 25% of the business (even indirectly). Where an ongoing business relationship is commenced, there is a requirement to obtain information regarding the purpose of any transactions, and the source of any funds.

7. CDD requirements must be carried out:
   - When establishing a business relationship
   - When carrying out an occasional transaction over €10,000 (or equivalent)
   - Where money laundering or terrorist financing is suspected
   - Where there are doubts about previously obtained customer information
   - As appropriate, for existing customers on a risk-sensitive basis
8. The vast majority of transactions completed by FLA motor finance members will usually fall into one of the above categories and therefore fall within the scope of CDD. The level of CDD measures must be taken on a risk sensitive basis, depending on the type of customer, business relationship or product.

SIMPLIFIED DUE DILIGENCE (SDD)

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

ENHANCED DUE DILIGENCE (EDD)

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

EVIDENCE OF IDENTITY

11. As standard under CDD, members must obtain for individuals:
   - full name
   - current residential address, and
   - date of birth

12. Members must obtain for business customers:
   - full name
   - registered number (if any)
   - registered office in company of incorporation
   - business address

13. Additionally for private or unlisted businesses:
   - Names of all directors
   - Names of all beneficial owners (to include ultimate beneficial owner or controlling person)

VERIFICATION OF IDENTITY

14. Members must verify customer identities through reliable and independent sources. This can be done through:
documents provided by the customer, or;
• electronic data, or;
• a combination of both.

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

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

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

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

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

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

ELECTRONIC VERIFICATION

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

NON-FACE-TO-FACE CUSTOMERS

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

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

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

   a. As soon as possible make available to it any information about the customer (and any beneficial owner) which the third party obtained when applying CDD/EDD measures.

   b. As soon as possible send it certified copies of standard proofs, identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third-party obtained when applying those measures.

   c. If the member relies on a 3rd party to complete checks, responsibility for completion of adequate CDD checks remains with the member and appropriate quality assurance procedures should be put in place.

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

BEST PRACTICE: GOING BEYOND THE FLA STANDARD

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

23. Private customers

   - **Obtaining an insurance certificate** from the customer to satisfy that the person insured to drive the vehicle is the same person listed on the finance agreement (and therefore no fronting has taken place). An insurance certificate would also reveal the level of excess the customer is subject to if they need to make a claim. Lenders can assess whether this falls within the terms and conditions of the agreement and that the level of excess is affordable.

   - **Asking the customer to share their driving licence details** using the DVLA’s Share Driving Licence service. This information will provide lenders with details which used to be provided on the paper counterpart. The service confirms that the driver has not been disqualified or has any medical conditions which prevent them from driving, or limitations to the vehicles they can drive. The customer would need to know their driver number, NI number and post code in order to share their driver record. The DVLA’s premium line service can also provide this information.

   - **Investigating the source of funds for any large deposits**, particularly those made above £10,000 and/or where such a deposit is out of keeping with the customer’s known financial status.

   - **Request self-employed trading accounts, SA302 and corresponding tax year overview or bank statements** if the customer does not hold a permanent job and an affordability check returns indifferent results.

   - **Verification of the customer on delivery of the vehicle** should be considered for non-face-to-face transactions. The vehicle could be delivered to a verifiable address associated with the
contract holder. It could then be handed over to the individual making/signing the agreement who can produce picture ID that appears valid and contains details that are consistent with previously supplied information.

24. Business customers

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

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

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

25. Supplier due diligence

- **Validating the supplier** to ensure the broker or dealer referring the customer is a legitimate business. Checks include:
  
  - Ensuring the business is FCA authorised or has interim permission by checking the Financial Services register.
  - Checking the website and company details.
  - Checking the address using web tools such as Google maps to confirm the external building looks like a valid business.
  - Contacting a business situated nearby to ask if the supplier are an active company.
  - Checking previous accounts information on Companies House (if not a new business) or those available from a Credit Reference Agency for corporate information.
Appendix 1

ACCEPTABLE EVIDENCE OF IDENTITY

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

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

Category 1
Face-to-Face Transaction

Definition

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

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

Examples

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

Identification Options

<table>
<thead>
<tr>
<th>Photo Identification</th>
<th>Know Your Customer / Prove Your Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Passport</td>
<td>➢ Passport</td>
</tr>
<tr>
<td>➢ Photo Card Driving Licence</td>
<td>➢ Photo Card Driving Licence</td>
</tr>
<tr>
<td>➢ National Identity Card</td>
<td>➢ National Identity Card</td>
</tr>
<tr>
<td>➢ HM Forces ID card</td>
<td>➢ HM Forces ID card</td>
</tr>
<tr>
<td>➢ Firearms certificate or shotgun licence</td>
<td>➢ Firearms certificate or shotgun licence</td>
</tr>
<tr>
<td>➢ Identity card issued by the Electoral Office for Northern Ireland</td>
<td>➢ Identity card issued by the Electoral Office for Northern Ireland</td>
</tr>
</tbody>
</table>

*Any of the above documents can be used on their own for Category 1 customers*

Or

<table>
<thead>
<tr>
<th>Non Photo Identification</th>
<th>Section 1</th>
<th>Section 2</th>
</tr>
</thead>
</table>

91
## Section 1

**Know Your Customer**

- Valid (old style) full UK driving licence
- Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant

**Prove Your Customer**

- Instrument of a court appointment
- Current council tax demand letter, or statement
- Current bank statement, or credit/debit card statement, issued by a regulated financial sector firm in the UK, EU or an assessed low risk jurisdiction
- Utility bills issued by a UK regulated electric, gas, water or telephone/mobile telephone provider

One document from Section 1 and one from section 2 is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below). Bank statements, council tax letters and bills must be current (date must be within the last 3 months).

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

Or

### Electronic Identification via an approved supplying agency

<table>
<thead>
<tr>
<th>Section 1</th>
<th>Section 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Know Your Customer</strong></td>
<td><strong>Prove Your Customer</strong></td>
</tr>
<tr>
<td>➢ One match on an individual’s full name and current address and ➢ A match on the individual’s full name and either his current address or his date of birth.</td>
<td>➢ Confirming the first payment to be carried out through an account confirmed in the customer’s name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction ➢ Knowledge Based Authentication questions ➢ Verify Debit/Credit Card in customers name and not stolen ➢ Send confirming letters to the customer’s verified address with either return information required, or passwords, internet log-ins etc. ➢ Any other credible and proven verification test that detects impersonation.</td>
</tr>
</tbody>
</table>

Examples of potential likely data matches are:
- Voters roll
- Public data e.g. CCJ
- Digital account information

The two sections need completing separately in order to comply

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

---

**Category 2**
Non-Face-to-Face Transactions with the Finance Company, but Face to Face customer contact with an FCA authorised motor dealer

Definition

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

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

Examples

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

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1</strong></td>
<td><strong>Section 2</strong></td>
</tr>
<tr>
<td>Know Your Customer</td>
<td>Prove Your Customer</td>
</tr>
<tr>
<td>➢ Passport</td>
<td>➢ Instrument of a court appointment</td>
</tr>
<tr>
<td>➢ Photocard Driving Licence</td>
<td>➢ Current council tax demand letter, or statement</td>
</tr>
<tr>
<td>➢ National Identity Card</td>
<td>➢ Current bank statement, or credit/debit card statement, issued by a regulated financial sector firm in the UK, EU or an assessed low risk jurisdiction</td>
</tr>
<tr>
<td>➢ Firearms certificate or shotgun licence</td>
<td>➢ Utility bills issued by a UK regulated electric, gas, water or telephone/mobile telephone provider</td>
</tr>
<tr>
<td>➢ Identity card issued by the Electoral Office for Northern Ireland</td>
<td>➢ Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant</td>
</tr>
<tr>
<td>➢ Valid (old style) full UK driving licence</td>
<td></td>
</tr>
<tr>
<td>➢ Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant</td>
<td></td>
</tr>
</tbody>
</table>

One document from each section above is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below). Bank statements, council tax letters and bills must be current (date must be within the last 3 months)

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

Or

Electronic Identification via an approved supplying agency
One match on an individual’s full name and current address
and
A match on the individual’s full name and either his current address or his date of birth.

Examples of potential likely data matches are:
- Voters roll
- Public data e.g. CCJ
- Digital account information

Confirming the first payment to be carried out through an account in the customer’s name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction

Knowledge Based Authentication questions

Verify Debit/Credit Card in customer’s name and not stolen

Send confirming letters to the customers verified address with either return information required, or passwords, internet log-ins etc.

The two sections need completing separately in order to comply

<table>
<thead>
<tr>
<th>Section 1</th>
<th>Section 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Know Your Customer</strong></td>
<td><strong>Prove Your Customer</strong></td>
</tr>
<tr>
<td>➢ One match on an individual’s full name and current address and</td>
<td>➢ Passport</td>
</tr>
<tr>
<td>➢ A match on the individual’s full name and either his current address or his date of birth.</td>
<td>➢ Photocard Driving Licence</td>
</tr>
<tr>
<td>Examples of potential likely data matches are:</td>
<td>➢ National Identity Card</td>
</tr>
<tr>
<td>o Voters roll</td>
<td>➢ HM Forces ID card</td>
</tr>
<tr>
<td>o Public data e.g. CCJ</td>
<td>➢ Firearms certificate or shotgun licence</td>
</tr>
<tr>
<td>o Digital account information</td>
<td>➢ Identity card issued by the Electoral Office for Northern Ireland</td>
</tr>
<tr>
<td>➢ Confirming the first payment to be carried out through an account in the customer’s name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction</td>
<td>➢ Valid (old style) full UK driving licence</td>
</tr>
<tr>
<td>Know Your Customer</td>
<td>Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant</td>
</tr>
</tbody>
</table>

One document from each section above is required, but they must be original documents - internet printed documents in pdf format are acceptable (see below).

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

Or

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

Category 3
Non-Face-to-Face Transactions, where the finance company, dealer or broker has had no face to face contact with the customer

Definition

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

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

Examples

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

Identification Options

<table>
<thead>
<tr>
<th>Electronic Identification via an approved supplying agency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1</strong></td>
</tr>
<tr>
<td>Know Your Customer</td>
</tr>
</tbody>
</table>

- One match on an individual’s full name and current address
- A match on the individual’s full name and either his current address or his date of birth.

Examples of potential likely data matches are:
- Voters roll
- Public data e.g. CCJ
- Digital account information

- Confirming the first payment to be carried out through an account in the customer’s name with a UK or EU regulated credit institution or one from an assessed low risk jurisdiction
- Knowledge Based Authentication questions
- Verify Debit/Credit Card in customer’s name and not stolen
- Send confirming letters to the customer’s verified address with either return information required, or passwords, internet log-ins etc.
- Any other credible and proven verification test that detects impersonation.

The two sections need completing separately in order to comply. Information from section 1 can include details provided through any form of correspondence with the customer or a third party.

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

- Verifying with the customer additional aspects of their identity (biometric data) which are held electronically;
- Requesting the applicant to confirm a secret PIN or biometric factor that links them incontrovertibly to the claimed identity.
- An additional verification check consisting of robust anti-fraud checks that members routinely undertake as part of their existing procedures (see Section 2 above).
11A: Consumer credit providers

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

Overview of the Sector

11A.1 Firms that undertake consumer credit businesses (but are not regulated for non-credit activities by the FCA before 1 April 2014) are subject to the provisions of the Money Laundering Regulations 2017, as they provide lending within point 2 of Schedule 2 of the ML Regulations. Some professional firms that provide consumer credit services and are subject to a designated professional body will not be required to be authorized, as they can take advantage of the FCA PROF Handbook, which means their compliance is overseen by their professional body.

11A.2 Certain consumer credit businesses (such as some pawnbrokers) which also undertake money service business activity, although authorised by the FCA for their consumer credit activity, will continue to be subject to supervision by HMRC. These businesses should follow HMRC guidance for the MSB sector but may find this guidance useful for their consumer credit activity.

11A.3 Consumer credit providers are therefore subject to the full provisions of UK law and regulation relating to the prevention of money laundering and terrorist financing. The guidance in Part I therefore applies to all consumer credit providers. Consumer credit providers are also subject to the FCA financial crime rules in SYSC 6.1.1 and 6.3.

Typical products

11A.4 Consumer credit providers covered by this guidance include both unsecured credit providers and secured lenders. Products provided include:

- Store cards and other revolving credit facilities
- Point of sale or other retail finance
- Personal loans or short term credit
- Second charge lending
- Secured loan provided by a pawnbroker

11A.5 The amounts lent are generally but not always under £25,000 and for periods of between 2-5 years (although some lenders provide larger value finance over longer terms for home improvements or for secured loans and substantially shorter for short-term, low value loans or interest free finance). This guidance will also be relevant to those businesses who sell goods or services on credit (although hire purchase is addressed in Sector 11: Motor Finance).

---

This applies where a consumer credit business falls within the definition of an “excluded money service business” in Regulation 22(5).

www.hmrc.gov.uk/mlr

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

But not first charge lending

There are no time constraints on revolving credit.
What are the money laundering or terrorist financing risks for consumer credit providers?

11A.6 With the exception of store cards or revolving credit facilities, the features of the lending are generally that the initial monies advanced are paid into the customer’s own or another bank account, e.g. the Point of Sale retailer. Repayments are usually made from the customer’s own bank or building society accounts by direct debit. Repayments in cash are not, and should not be, encouraged.

11A.7 Generally, consumer credit providers do not hold permission from the FCA to handle client money (although other parts of the businesses may do if they are part of larger retail banking groups), so in practice there is unlikely to be any involvement in the placement stage of money laundering. There is, however, scope for consumer credit providers to be drawn in to the layering and integration stages.

11A.8 The main money laundering risks arise through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination or settlement. Consumer credit providers should be aware that early repayments carry a risk that the funds have emanated from a criminal lifestyle.

11A.9 Overall, however, the provision of consumer credit carries a low inherent money laundering/terrorist financing risk. Lenders will normally only accept payment of instalments from the customer named on the agreement, and in the case of an overpayment will only make repayment to the customer named on the agreement.

11A.10 However, if a consumer credit provider accepts occasional payments from third parties, for example, on settlement of the agreement, it must be alert to the unknown nature of the source of these funds, which may increase the risk of receiving the proceeds of crime. There is also a risk for pawnbrokers providing a secured loan, that the goods held as security may be the proceeds of crime.

Assessment of the risk

11A.11 For single advance finance, the lender’s knowledge of the customer (other than an existing customer) only extends to information gleaned at the identification stage, and to a single monthly payment on the agreement. Their occupation details and income are generally known and the applicant’s details are usually validated by searches at one or more of the Credit Reference Agencies.

11A.12 For Store cards and revolving credit facilities, additional reviews are undertaken on a regular basis to update the customer details.

11A.13 The nature of consumer credit, however, is that the type of agreement entered into with the customer carries a relatively low risk of money laundering.

11A.14 Consumer credit can be provided through a number of different channels. Customers may be introduced through the internet, via the telephone, by post or face to face. Where lending is obtained remotely without face-to-face contact, this is likely to carry a higher risk.

11A.15 Procedures and controls used for identifying potential money laundering are therefore normally transactional-based, to identify unusual transactional movements, unusual deposits, unusual advance payments or unusual repayment patterns.

Customer Due Diligence (CDD)

11A.16 Having sufficient information about customers and beneficial owners and using that information underpins all other anti-money laundering procedures. A firm must not enter into
a business relationship until the identity of all the relevant parties to the relationship has been verified in accordance with the guidance in Part I, Chapter 5.

11A.17 The borrower in respect of consumer credit tends to be a private individual, although loans of these types can be made for business purposes to sole traders and partnerships of two or three partners (not all of whom are corporate entities). If the borrower is a large partnership, a limited liability partnership or a private or public company, the borrowing will not be regulated by the Consumer Credit Act 1974 but the business must obtain information that is relevant to that entity such as company registration number and registered address. For all business entities, it is prudent to obtain (where relevant) evidence that individuals have the authority to act for that entity and evidence to establish beneficial owners of such entities.

11A.18 Further guidance on identification and verification of the customer is given in Part I 5.3.2-5.3.7. Further detail on identification and verification of a beneficial owner is available at 5.3.8-5.3.13. Guidance on the requirements relating to existing customers is set out in Part I at 5.3.14-5.3.17.

Private individuals

11A.19 Guidance on verifying the identity of private individual consumers is given in Part I, paragraphs 5.3.57 to 5.3.105. This validation may be undertaken by either the lender or by a broker e.g. for Point of Sale Finance. However, where such a broker is not regulated by the FCA in its own right, it is important to recognize that it may be acting merely as an authorised representative of the lender (see Part I, paragraphs 5.6.34-5.6.43).

11A.20 Customers may be assessed as presenting a higher risk of money laundering if they are identified as being Politically Exposed Persons (PEPs), or because of some other aspect of the nature of the customer, or his business, or its location, or because of the product features available. In such cases, the firm must conduct enhanced due diligence measures (see Part I section 5.5) and will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity. For such customers, the lender will need to consider whether to require additional customer information (see Part I, section 5.5) and/or whether to institute enhanced monitoring (see Part I, section 5.7).

11A.21 Non face-to-face transactions can present a greater money laundering or terrorist financing risk than those conducted in person because it is inherently more difficult to be sure that the person with whom the firm is dealing is the person that they claim to be. Enhanced due diligence is required in these circumstances, and verification of identity undertaken on a non-face-to-face basis should be carried out in accordance with the guidance given in Part I, paragraphs 5.5.10 to 5.5.17.

11A.22 Some persons may not be able to produce the standard evidence of identity. Where customers cannot produce the standard identification of evidence, reference should be made to the guidance set out in sector I: Retail banking, Annex I-I.

Non Personal Customers

11A.23 Guidance on verifying the identity of non-personal customers is given in Part I, paragraphs 5.3.106 to 5.3.168. Categories of non-personal customers that are likely to be of particular relevance to consumer credit providers are:
- small partnerships and unincorporated businesses (paragraphs 5.3.154-5.3.168)

11A.24 Consumer credit providers may also want to refer to Part II, Sector 11: Motor finance, Annex 11-I sections 1-6. This documents the Industry Standards for Fraud Prevention in Credit Application Processing. This documents standard identification evidence. It should be noted
that some of the requirements set out in this industry standard exceed those now required for lower risk products under the current money laundering regulations.

*Using verification work carried out by another firm*

11A.25 The responsibility to be satisfied that a customer’s identity has been verified rests with the firm entering into the transaction with the customer. However, where two or more financial transaction, in certain circumstances one firm may use the verification carried out by another firm. Guidance on the circumstances in which such an approach is possible, and on the use of pro-forma confirmation documentation, is given in Part I, section 5.6.

11A.26 Consumer credit providers should bear in mind that they are often the party which is carrying out the initial customer identification and verification process.

*Suspicious transactions*

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

*Staff awareness and training*

11A.28 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions, which may prove to be suspicious.

11A.29 Guidance on staff awareness, training and alertness is given in Part I, Chapter 7. This guidance includes suggested questions that staff should be asking themselves, and circumstances that should cause them to ask further questions about particular transactions or customer activity.

*Record-keeping*

11A.30 General guidance on record-keeping is given in Part I, Chapter 8. Verification of the identity of a customer or beneficial owner may be by means of documentation or electronically. Where documents are used, it is preferable to make and retain copies.

11A.31 Documents relating to customer identity must be retained for five years from the date the business relationship with the customer has ended (see Part I, paragraph 8.12).
16: Correspondent Relationships

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

This sectoral guidance considers specific issues over and above the more general guidance set out in Part I, Chapters 4, 5, and 7, which firms engaged in Correspondent Banking Relationships or Correspondent Trading Relationships should take into account when considering applying a risk-based approach.

Overview of the sector

16.1 Under the ML Regulations, all relationships with Credit and Financial Institutions fall within the definition of Correspondent Relationships. For the purposes of this guidance, however, a distinction is drawn between banking and trading relationships, given the different risks and method of operation. This is reflected in the way that due diligence measures should be applied. Collectively, Correspondent Banking and Correspondent Trading relationships will be referred to as “Correspondent Relationships”.

16.2 Correspondent Relationships covers:

- **Correspondent Banking Relationships.** A “Correspondent Banking Relationship” is the provision of banking-related services by one bank (Correspondent) to another bank (Respondent) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network.

  Correspondent Banking Relationships can include establishing accounts, exchanging methods of authentication of instructions (e.g. by establishing SWIFT RMAs) and providing payment or other clearing-related services. 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.

- **Correspondent Trading Relationships.** A “Correspondent Trading Relationship” is a relationship among credit institutions or financial institutions for the provision of commercial or business products or services—which may include relationships established for securities transactions or funds transfers, including services within the scope of Chapter 18 – Wholesale markets or Chapter 17 – Syndicated Lending, or which could simply be the provision of loan finance from one credit or financial services institutions to another. Such relationships may be described as a bilateral commercial arrangement between two institutions, rather than the provision of Correspondent Banking Relationship-related services from one institution to another (as defined above). These relationships do not have a Correspondent and a Respondent since neither party is providing services on behalf of the other or for an underlying customer; accordingly, the degree of ML/TF risk in such relationships is different, generally lower, than it is with relationships which provide for banking-related services on behalf of that institution’s customers. They are more similar to normal customer relationships.
16.3 Generally, in a Correspondent Banking Relationship, a Correspondent is effectively an agent (intermediary) for the Respondent and executes/processes payments or other transactions for customers of the Respondent. The underlying customers may be individuals, corporates or even other financial services firms. Beneficiaries of transactions can be customers of the Correspondent, the Respondent itself or, in many cases, customers of other banks and therefore unknown.

What are the money laundering risks in Correspondent Relationships?

16.4 The Correspondent often has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities. Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments (wire transfers – see Part 1, paragraph 5.2.10 - 5.2.13) or clearing cheques.

16.5 For these reasons, Correspondent Relationships are, in the main, non face-to-face business and, when an unknown third party is involved, must be regarded as potentially high risk from a money laundering and/or terrorist financing perspective.

16.6 Correspondent Banking Relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CTF systems and controls, and customers of those firms, direct access to international banking systems.

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

16.8 The degree of ML/TF risk presented by different types of Correspondent Relationships between firms will vary, sometimes considerably – for example, some relationships cannot result in payments being made, which clearly carries an almost non-existent degree of risk – and, therefore, the appropriate customer due diligence measures that should be applied will similarly vary, according to the assessed degree of risk.

16.9 The primary risk in Correspondent Relationships turns on whether a relationship or transaction is between financial or credit institutions as principal, where the risks are inherently low, especially where the counterparty is based within the EEA (or an assessed low risk jurisdiction). Where the transaction relates to an underlying customer or customers – if this is disclosed, the Correspondent will know who it is dealing with, if undisclosed, this will heighten the risk.

How to assess the elements of risk in Correspondent Banking Relationships

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

- deal or trade on behalf of undisclosed customers; or
- are offshore banks that are limited to conducting business with non-residents or in non-local currency, and are not subject to robust supervision of their AML/CTF controls; or
- are domiciled in jurisdictions with weak regulatory/AML/CTF controls or other significant reputational risk factors e.g., corruption.

16.11 The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken. These risks are particularly relevant for Correspondent Banking Relationships:
16.4 **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.

16.5 **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.

16.6 **The Respondent’s business and customer base.** The type of business the Respondent engages in, as well as the type of markets it serves, is indicative of the risk the Respondent presents. Involvement in certain business segments that are recognised internationally as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a Respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as activities or countries being especially susceptible of money laundering/terrorist financing or corruption. Equally, a Respondent that has a predominantly low risk customer base, and/or is based in a well-regulated jurisdiction with high AML/CFT standards, carries a much lower risk.

16.7 **Downstream Correspondent Clearing.** A Downstream Correspondent Clearer is a Respondent that receives correspondent banking services from a Correspondent and itself provides correspondent banking services to other financial institutions in the same currency as the account it maintains with its Correspondent. When these services are offered to a Respondent that is itself a Downstream Correspondent Clearer, a Correspondent should, on a risk-based approach, take reasonable steps to understand the types and risks of financial institutions to whom the Respondent offers such services, especial care being taken to ensure there are no shell bank customers, and consider the degree to which the Respondent examines the anti-money laundering/terrorist financing controls of those financial institutions.

16.12 Other factors that might affect the Respondent’s risk profile include whether:

- the Respondent, their parent or a firm belonging to the same group as the Respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations

- the history of the business relationship with the Respondent gives rise to concern, for example because the amount of transactions are not in line with what the Correspondent would expect based on their knowledge of the nature and size of the Respondent.

16.13 The following factors may indicate lower risk:
the Respondent is based in an EEA Member State.

The Respondent is based in a third country which has AML/CFT requirements that are consistent with the 2012 FATF Recommendations and effectively implements those requirements.

the relationship is limited to a SWIFT RMA plus capability, which is designed to manage communications between financial institutions. This means that the respondent, or counterparty, does not have a payment account relationship.

the banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying clients, e.g. foreign exchange services between two banks where the business is transacted on a principal to principal basis between the banks, and where the settlement of such a transaction does not involve a payment to an unknown third party.

Correspondents must not maintain relationships with Respondents that are shell banks (see Part I, paragraphs 5.3.54 – 5.3.56) nor with any Respondent which provides banking services to shell banks.

How to assess the elements of risk in Correspondent Trading Relationships

The degree of risk in a Correspondent Trading Relationship should be determined bearing in mind the risks inherent in the product and service, and the risks posed by the nature and jurisdictions of operation of the counterparty, in particular whether or not unknown third parties are involved. The risk assessment will essentially follow the firm’s standard approach.

Customer due diligence

The customer due diligence measures to be carried out in relation to Correspondent Relationships depends on the particular type of relationship established, where the counterparty is based, and the degree of risk of money laundering or terrorist financing presented by the relationship.

All Correspondent Relationships must be subject to an appropriate level of due diligence which:

- meets the firm’s standard customer due diligence requirements, reflecting the degree of risk determined in the relationship, and;
- ensures that the firm is comfortable conducting business with/for a particular counterparty (and, if applicable, its underlying customers) given the counterparty’s risk profile.

For counterparties based in an EEA Member State, the firm will follow its standard customer due diligence procedures, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the firm to apply CDD, SDD or EDD measures in accordance with the guidance in Part I, Chapter 5.

It will be appropriate for a firm to take account of the fact that a counterparty firm is domiciled or operating in a regulatory environment that is recognised internationally as adequate in the fight against money laundering/terrorist financing and corruption. In these instances, a firm may choose to rely on publicly available information obtained either from the counterparty itself, from another reputable existing counterparty, from other credible sources (e.g., regulators, exchanges), or from reputable information sources (e.g. SWIFT KYC Registry), to satisfy its due diligence requirements.
16.20 The extent of the Correspondent Relationship should be factored into the level of due diligence undertaken. A firm, under its risk-based approach, may decide to undertake the minimum level of due diligence set out in Regulation 28 for limited correspondent relationships, such as those limited to a SWIFT RMA plus capability, or for Correspondent Trading Relationship transactions undertaken within the UK or the EEA on a bilateral basis.

16.21 A firm’s policies, controls and procedures should require that the information, including due diligence, held relating to the counterparty to its Correspondent Relationship is periodically reviewed and updated. The frequency of review should be tailored to the assessed degree of risk, and updating should be undertaken as a result of trigger events e.g. an extension to the service/product range provided; a material change to the nature/scope of business undertaken by the Respondent; or as a result of significant changes to its legal constitution, or its owners or controllers or negative regulatory pronouncements and/or press coverage.

16.22 In respect of Correspondent Banking Relationships, the level and scope of due diligence undertaken should take account of the relationship between the Respondent and its ultimate parent (if any). In general, for relationships maintained with branches, subsidiaries or affiliates, the status, reputation and controls of the parent entity should be considered in determining the extent of due diligence required on the Respondent. Where the Respondent is located in a high-risk jurisdiction, Correspondents may consider it appropriate to conduct additional due diligence on the Respondent as well as the parent. In instances when the Respondent is an affiliate that is not substantially and effectively controlled by the parent, then the quality of the affiliate’s AML/CTF controls should always be established.

The Correspondent, in assessing the level of due diligence to be carried out in respect of a particular Respondent, (in addition to the issues raised in paragraph 16.11) must consider:

### 16.24 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.

### 16.25 AML/CTF controls

A Correspondent should establish whether the Respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the Respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in the Fourth Money Laundering Directive. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the Respondent’s internal policy on money laundering/terrorist financing prevention and its knowledge of customer and activity monitoring controls and procedures. Where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in the Fourth Money Laundering Directive. If not, the extent to which the parent’s controls meet FATF standards/equivalent to those laid down in the money laundering directive and whether these are communicated and enforced ‘effectively’ throughout its network of international offices, should be ascertained.

16.23 Correspondent Relationships with shell banks are prohibited in all circumstances and so the firm should satisfy itself that its counterparty is not a shell bank. Firms must also take appropriate measures to ensure that they do not enter into, or continue, a correspondent relationship with a credit institution or financial institution which is known to allow its accounts to be used by a shell bank.
16.24 Where a counterparty based in a third country is a branch or subsidiary undertaking of a credit or financial institution in an EEA state, the firm should on a risk based approach consider the extent to which EDD measures should be applied. The risk presented by such a customer may be mitigated where they are subject to Group AML/CTF standards that are compliant with the ML Regulations or the EU Fourth Money Laundering Directive and the parent entity is EEA regulated.

**Enhanced due diligence for Correspondent Relationships**

16.25 The ML Regulations prescribe that EDD measures are required to be carried out in respect of Correspondent Relationships with Respondents based in non-EEA jurisdictions. For Respondents based in EEA Member States, the firm’s risk assessment will require EDD measures to be applied if the firm determines that the relationship presents a higher degree of ML/TF risk.

16.26 Firms need to ensure appropriate EDD requirements are applied to non-EEA counterparties. When considering whether a counterparty should be treated as an EEA institution or a non-EEA institution the relationship should be assessed at the regulated firm level, rather than at the legal entity level. Firms should ensure that they fully document their decision-making process.

In meeting the prescribed EDD requirements for non-EEA counterparties, a firm should consider the following matters when interpreting how each requirement is applied, and The firm should document their decision-making process. When considering whether or not a counterparty is an EEA institution or a non-EEA institution, for UK or EEA branches or subsidiary undertakings of non-EEA banks, where such branch or subsidiary undertaking is authorised and regulated in the UK or EEA, these matters should be assessed at regulated firm level, rather than legal entity level.

16.27 Firms should identify whether they are entering into a Correspondent Banking or Correspondent Trading relationship. A Correspondent Banking Relationship is typically higher risk and therefore firms must apply the Enhanced Due Diligence measures in full. By contrast, a Correspondent Trading Relationship, and in particular those where no unknown third party is involved, may be lower risk. In applying EDD measures; however, firms must decide on the precise measures to be applied on a risk sensitive basis.

**Enhanced due diligence for Correspondent Banking Relationships**

16.28 The following EDD measures should be considered for Correspondent Banking Relationships:

- **Nature of Business.** Firms must gather sufficient information about the Respondent to understand fully the nature of its business. The amount of information gathered on the customer may be on a risk based approach and may take into consideration the following (non-exhaustive list):
  - Type of Respondent – an assessment of the credit or financial institution type
  - Business Model – the customer base of the Respondent and the products and services it offers
  - Country of operations – is the Respondent based in a non-EEA country, which has AML/CTF requirements which are equivalent to the ML Regulations and/or the fourth money laundering directive?
  - Does the Respondent have operations in high risk jurisdictions?

- **Reputation and Supervision.** Firms must determine using credible, publicly available information, the reputation and supervision of the Respondent. Firms should have regard to the following:
The disciplinary record of the Respondent – Has the Respondent been subject to recent regulatory enforcement for inadequate AML/CTF systems and controls?

- Regulated status of the Respondent – Whether the respondent is regulated
- AML Regime – is the Respondent based in a non-EEA country with an effective AML/CTF regime?
- Jurisdiction in which the Respondent is regulated - whether the respondent is subject to adequate AML / CTF Supervision

### Assessment of the Firm’s AML / CTF Controls

Firms must assess the Respondent’s AML / CTF framework. This may be applied on a risk based approach, with a varying degree of scrutiny depending on the risks identified as part of the Enhanced Due Diligence process. Firms may also wish to leverage established industry questionnaires or similar to meet this requirement. Additionally, the Correspondent may wish to speak with representatives of the Respondent to obtain comfort that the Respondent’s senior management recognise the importance of anti-money laundering/terrorist financing controls.

### Senior Management Approval

Firms must obtain senior management approval before establishing a new Correspondent Banking Relationship. The firm should determine who constitutes “senior management” for the purposes of the Correspondent Banking Relationship approval process. However, the approver should have sufficient knowledge of the firm’s AML / CTF risk exposure, and of sufficient authority to take decisions affecting the firm’s risk exposure. Firms should document internally their approach to customer relationship approvals and should have a sliding scale of approvals depending on the risk of the customer relationship.

A new Correspondent Banking Relationship refers to the initial onboarding of the customer. However, firms should consider, on a risk based approach whether any further senior management approvals might be required by the risk profile of the new product and / or business line being offered and in accordance with the Firms risk assessment of the business.

### Responsibilities of the Respondent and Correspondent

Firms must document the responsibilities of the Respondent and Correspondent. In some instances this information may be contained within contractual language (including terms of business) between the Correspondent and Respondent.

### Direct Access to Correspondent Accounts

Firms must identify whether the Respondent’s customers have access to their accounts. If the Respondent’s customers have access, the Correspondent must be satisfied that:

- The Respondent has verified the identity of, and conducts relevant completed CDD checks on their customers on an ongoing basis
- The Respondent is able to provide upon request the CDD data or information gathered

### SWIFT (RMA) relationships

Due diligence should take into account the message types being made available to the respondent bank. Message types Category 1 and Category 2 bring heightened risks and, therefore, enhanced due diligence must be considered in these circumstances.

### Shell banks

Whether the Respondent has confirmed that it will not provide banking services to, or engage in business with, shell banks
16.29 The enhanced due diligence process for Correspondent Banking Relationships should involve further consideration of the following elements designed to ensure that the Correspondent has secured a greater level of understanding:

16.29.1 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).

16.10. 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.

16.11 PEP involvement. If a PEP (see Part I, paragraphs 5.5.1-5.5.31) appears to have a material interest or management role in a Respondent then the Correspondent should ensure it has an understanding of that person’s role in the Respondent.

Enhanced due diligence for Correspondent Trading Relationships

16.30 In relation to Correspondent Trading Relationships, a firm will apply its standard customer due diligence approach, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the firm to apply CDD, SDD or EDD measures in accordance with the guidance in Part I, Chapter 5.

16.31 Due to the inherently lower risk profile of many Correspondent Trading Relationships, a firm should take the following measures in order to meet the prescribed enhanced due diligence requirements of the ML Regulations relating to Correspondent Trading Relationships with non-EEA based respondents (in addition to its standard customer due diligence approach, based on its determination of the ML/TF risk presented following its risk assessment):

- ensure that the other institution is clearly identified on the firm’s records as being the counterparty to the transaction;
- gather information about the nature of the business of the other institution;
- include the institution in the firm’s regular customer screening for PEPs, sanctions and other financial crime indicators and follow the same approach as for other customers in terms of assessing and applying the results of such screening within the firm’s risk-based approach;
- satisfy itself that the other institution is authorised and regulated in a non-EEA country which has AML/CTF requirements which are equivalent to the ML Regulations and/or the EU Fourth Money Laundering Directive (and the country receiving an EU or UK equivalence ruling would be sufficient evidence of this), or otherwise undertake an assessment of the other institution’s AML/CTF framework. This may be applied on a risk-based approach, with a varying degree of scrutiny depending on the risks identified as part of the EDD process. Firms may also wish to leverage established industry questionnaires or similar to meet this requirement including a determination of the respondent’s reputation.
16.32 Where a firm identifies additional risk or is not able to satisfy the measures set out in 16.31, it should consider what further due diligence measures would be appropriate to mitigate the additional risk.

### Monitoring of Correspondent Banking Relationships

16.33 Implementing appropriate documented monitoring procedures can help mitigate the money laundering risks for firms undertaking correspondent banking activities. General guidance on monitoring is set out in Part 1, section 5.7.

16.34 The level of monitoring activity undertaken by a Correspondent on its Respondent’s activity through it should be commensurate with the risks determined to be posed by the Respondent. Due to the significant volumes that correspondent banking activity can entail, together with the need to work within prescribed scheme settlement deadlines, electronic and/or post-execution monitoring processes are often the norm.

16.35 The following techniques should be considered where relevant for monitoring activity in the area of Correspondent Banking Relationships:

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

- **Hidden relationships**
  - Monitor for activity between accounts, customers (including Respondents and their underlying customers). Identify common beneficiaries and remitters or both amongst apparently unconnected accounts/Respondents. This is commonly known as link analysis.

- **High risk geographies and entities**
  - Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk geographies and/or entities.
➢ Other money laundering behaviours
   • Monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds, or transactions in round amounts

➢ Other considerations
   In addition to the monitoring techniques above, the monitoring system employed to monitor correspondent banking for AML/CTF purposes should facilitate the ability to apply different thresholds against customers that are appropriate to their particular risk category.

16.36 In addition to monitoring account/transaction activity, a Correspondent should monitor a Respondent for changes in its nature and status. As such, information about the Respondent collected during the customer acceptance and due diligence processes must be:

➢ Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis), or
➢ Reviewed on an ad hoc basis as a result of changes to the customers information identified during normal business practices, or
➢ Reviewed when external factors result in a material change in the risk profile of the customer.

16.37 Where such changes are identified, the Respondent should be subject to a revised risk assessment, and a revision of their risk categorisation, as appropriate. Where, as a result of the review, the risk categorisation is altered (either up or down) a firm should ensure that the due diligence standards for the Respondent’s new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

16.38 Firms should consider terminating the accounts of Respondents, and consider their obligation to report suspicious activity, for Respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers featuring in unusual or suspicious transactions or activities.

16.39 The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:

- Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
- Adequacy of staff training and awareness;
- Capturing appropriate management information;
- Upward reporting and accountability; and
- Effectiveness of liaison with regulatory and law enforcement agencies.

Staff awareness, training and alertness in respect of Correspondent Banking Relationships

16.40 Where the firm is a Correspondent, the firm must train staff on how correspondent banking transactions may be used for ML/TF and in the firm’s procedures for managing this risk. This training should be directed specifically at those staff directly involved in correspondent banking transactions and dealing with correspondent banking clients and should be tailored around the greater risks that this type of business represents.
16.41 Firms should provide “senior management” approving correspondent relationships with appropriate training to provide them with sufficient knowledge of the firm’s money laundering and terrorist financing risk exposure.

*Monitoring and staff awareness, training and alertness in respect of Correspondent Trading Relationships*

16.42 The monitoring and staff awareness, training and alertness principles set out in Part I of this Guidance would be applicable.
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 I, Chapters 4, 5, and 7, which firms operating in the wholesale markets may want to take into account when considering applying a risk-based approach. Firms may also find the guidance for the following sectors useful:

➢ Sector 8: Non-life providers of investment fund products, which deals with exchange-traded products where the firm acts as agent for private customers, (e.g. where a fund provider that is not an exchange member buys securities for its private customers).

➢ Sector 9: Discretionary and advisory investment management, which covers how investment managers may interact with wholesale markets.

➢ Sector 10: Execution-only stockbrokers, which will be more relevant for firms dealing in wholesale market products as agent or principal for retail customers.

➢ Sector 14: Corporate finance, which deals with the issuance of traded products or instruments, which are traded in a ‘secondary’ wholesale market, allowing investors in the primary market to realise their investment.

➢ Sector 16: Correspondent Relationships, which deals with business relationships between firms.

➢ Sector 17: Syndicated lending, which primarily deals with the syndication of loans and trading on the secondary market.

➢ Sector 19: Name Passing Brokers, which is directed at those firms who deal with wholesale market brokers in the inter-professional markets.

➢ Sector 20: Brokerage Services to Funds, which is intended for firms who are involved in multipartite relationships in respect of, and/or provide services, including the execution and clearing of transaction in wholesale market products to, unregulated funds.

A. Overview of the sector

18.1 The wholesale markets comprise exchanges and dealing arrangements that facilitate the trading (buying and selling) of wholesale investment products, and hedging instruments (“traded products”), including, but not limited to:

➢ Securities: equities, fixed income, warrants and investment funds (Exchange Traded Funds – ETFs);

➢ Money market instruments: FX, interest rate products, term deposits;

➢ Financial derivatives: options, futures, swaps and warrants;

➢ Commodities: physical commodities and commodity derivatives, including exotic derivatives (e.g., weather derivatives); and

➢ Structured products (e.g., equity linked notes).

18.2 This guidance provides general guidance on assessing risks in wholesale markets, due diligence and monitoring. It then provides additional guidance on each of the product types referred to above. Reference should be made to both the general and the relevant product-specific guidance in this section, as well as to the general guidance in Part I.

18.3 Traded products confer ‘rights’ or ‘obligations’; either between an investor and the issuer, or between parties engaged in the trading of the instruments. Traded products can be bought, sold, borrowed or lent; as such, they facilitate the transfer of property or assets and usually represent
an intrinsic value, which may be attractive to money launderers. Traded products can be bought or sold either on an exchange (“exchange traded products”), or between parties “over-the-counter” (“OTC”).

18.4 Some traded products or instruments, such as equities, are issued in a ‘primary’ market, and are traded in a ‘secondary’ market, allowing investors in the primary market to realise their investment. Other traded products are created to enable investors to manage assets and liabilities, exchange risks and exposure to particular assets, commodities or securities.

Role of the parties

18.5 The following are persons typically involved in wholesale market activities:

- **Instructing Counterparty**: The customer on whose behalf the transaction or trade is being conducted;
- **Agent**: An agent in the context of the wholesale markets is an entity which provides related financial services for or on behalf of a customer;
- **Executing Broker**: An executing broker is the broker or dealer that finalises and processes an order to transact/trade on behalf of a customer;
- **Clearing Broker**: A clearing broker settles transactions/trades on behalf of the customer and as such will handle the movement of funds or assets for the customer in settlement of respective transactions and liabilities;
- **Central Counterparty (CCP)**: A CCP is an organisation that exists to help facilitate trading activities on certain markets by providing efficiency and stability as a financial intermediary to a transaction/trade;
- **Custodian**: A custodian is a financial institution that holds a customer’s securities for safekeeping and protection; and
- **Investment Manager or Adviser**: Funds are managed by an investment manager, which is a separate legal entity from the fund, and which is given authority to act as agent and manage the funds and investments held by the fund vehicle. It is often the investment manager that will make investment decisions and place transactions with a firm as agent of the fund. The investment manager may delegate certain activities to a separate Investment Adviser.

**Exchange-traded products**

18.6 Exchange-traded products are financial products that are traded on exchanges, which have standardised terms (e.g. amounts, delivery dates and terms) and settlement procedures and transparent pricing. Firms may deal in exchange-traded products as principal or as agent for their customers. In the financial and commodity derivatives markets, firms will typically deal as principal, and on certain exchanges (e.g. Euronext.LIFFE, ICE Futures, LME) must do so when dealing as a clearing member in relation to their customers’ transactions. In the securities markets, firms can deal as either principal or as agent for the firms’ underlying customers.

18.7 The London Stock Exchange recognises different types of relationships between a settlement agent and its customers, which it denotes as Model A and Model B. Similar relationships may be recognised on other exchanges and different terminology used to denote these relationships.

18.8 Most exchanges have a CCP which stands between the exchange members that are buying and selling a product (becoming the buyer to the seller and the seller to the buyer). Where an exchange or trading platform does not have a CCP, the members contract with each other.
OTC products

18.9 OTC products are bilateral agreements between two parties (or may be multilateral agreements, depending on the settlement process), that are not traded or executed on an exchange. The terms of the agreement are tailored to meet the needs of the parties, i.e., there are not necessarily standardised terms, contract sizes or delivery dates. Where firms deal OTC, they usually deal as principal. Some OTC dealing is facilitated by brokers and, while settlement is normally effected directly between the parties, it is becoming increasingly common for exchanges and clearers to provide clearing facilities (i.e., the trades are executed as OTC but are then given up for clearing by a CCP).

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

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

18.11 However, the characteristics of traded products, which facilitate the rapid and sometimes opaque transfer of ownership, and the ability to change the nature of an asset and market mechanisms that potentially complicate the audit trail, together with a diverse international customer base, present specific money laundering risks that need to be addressed and managed appropriately. [Note: the "National risk assessment of money laundering and terrorist financing 2017" has been taken into account when updating this chapter and this guidance is considered to accord with the provisions of that document.]

18.12 Given wholesale markets’ global flows of funds, speed of transactions and potential ease of converting holdings to cash, they are capable of being used for money laundering, but it is important to recognise that these markets may be abused by criminals at different stages of the money laundering process and that the risks of money laundering in the wholesale markets may vary, depending upon the products and services a firm offers to a customer. It is important for a firm to understand at which stage(s) risks may arise (and this may vary from firm to firm):

➢ Placement: It is unlikely that physical currency or bearer instruments could be placed into the wholesale financial markets, as the primary acceptance of such assets is not a service offered by firms carrying out business in the UK within this sector.

➢ Layering: The wholesale financial markets grant the means to execute and clear a chain of transactions which may be complex, involving a multitude of financial instruments and/or financial institutions. This environment may potentially be abused by a criminal to layer funds and/or asset ownership with an aim of obfuscating the illicit origin of such funds/assets. Methods such as ‘mirror trading’, ‘wash trading’ or ‘offsetting transactions’ have been identified by the FCA as having been utilised in a manner highly suggestive of financial crime20. A firm should also consider whether it facilitates the electronic transfer of funds into the wholesale market sector from an outside source, particularly from a third party or jurisdiction considered to present a higher risk for money laundering.

➢ Integration: Some financial instruments transacted on the wholesale markets can be rapidly liquidated to cash or reinvested into other holdings. A firm may then facilitate the further integration of these funds through the purchase or transfer of other existing assets. Whilst these activities are generally legal and legitimate, firms should consider the associated and varied money laundering risks when a customer instructs the transfer of value (by payment or change of asset ownership) to an overseas jurisdiction, particularly where a third party is involved.

➢ Post-integration (use of criminal proceeds): It can be very difficult to identify proceeds of crime once they have been integrated and mixed with legitimate funds in wholesale market products. Once proceeds of crime have been integrated in this way, it is likely that only the firm whose customer is the end party (and which would therefore have carried out customer

due diligence ("CDD") on that party would be in a position to potentially identify such proceeds, by identifying any irregularity/inconsistency between the value of the transaction and its customer’s source of wealth or funds (although such inconsistencies may, even then, be difficult to identify). Where the end party already has significant legitimate wealth, the use by that party of the proceeds of crime for investment purposes (rather than further layering of funds) will, again, be difficult to identify, even by the firm which has conducted CDD on that party as its customer.

Firms dealing in traded products in the wholesale markets do not generally accept cash deposits or provide personal accounts that facilitate money transmission and/or third party funding that is not related to specific underlying investment transactions. Third party payments may, however, be used in relation to particular products, such as FX and/or commodities. Firms should consider whether third party payments are possible and whether the ability to make such payments presents additional money laundering risks, and should have regard to the product-specific guidance in this chapter where relevant.

The extent to which certain products are subject to margin or option premium payment arrangements will affect the level of risk. The nature and form of any margin will need to be taken into account by the firm, through its risk-based approach, when identifying the customer and determining appropriate payment procedures.

OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in assessed lower risk jurisdictions, are transparent and have a CCP to clear trades, can ordinarily be seen as carrying a lower generic money laundering risk. OTC business will, generally, be less transparent, and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. For example, exchanges often impose specific requirements on position transfers, which have the effect of reducing the level of money laundering risk. These procedures will not apply in the OTC markets, where firms will need to consider the approach they would adopt in relation to any such requests in respect of customers dealing OTC. Trades that are executed as OTC but then are centrally cleared may have a different risk profile to trades that are executed and settled OTC. Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

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

The main factors to consider when assessing the risk when undertaking business in the wholesale markets are: the nature of the customer; the market participants; the products involved; and whether the products are exchange traded or OTC.

When implementing a risk-based approach, producing or reviewing risk assessments, or assessing the risk profile of a prospective customer, there are a number of areas which firms may want to take into account in addition to the more general matters set out in Part I, Chapters 4 and 5.

➢ The wholesale markets are populated by customers with a wide range of different business interests. The types of participants present might typically include, but are not limited to:
  • Sovereign governments;
  • Local authorities (municipal bodies);
  • Regulated financial firms (e.g. banks, brokers, investment managers and funds);
  • Unregulated financial entities (e.g. off-shore funds);
  • Corporations (e.g. listed companies, private companies); or
  • Trust and partnerships.
➢ A customer’s nature, status, and the degree of independent oversight to which it is subject may affect the firm’s assessment of risk for the particular customer or for the firm's business as a whole.

➢ The instruments traded in the wholesale markets can allow for long-term investment, speculative trading, hedging and physical delivery of certain financial instruments and commodities. Understanding the role of a prospective customer in the market, and the customer's reasons for trading, will help inform decisions on the risk profile the customer presents.

➢ The way that a firm addresses the jurisdictional risk posed by a customer will depend on a number of factors. Jurisdictional risk should be considered but may, in relevant cases, be mitigated by the rationale for the customer being located or operating in a particular jurisdiction; customers located in potentially higher risk jurisdictions may have legitimate commercial interests which can mitigate the perceived risk, and presence in a higher risk jurisdiction does not necessarily render a customer high risk for AML/CTF purposes. For example, an oil producer in a higher risk territory may seek to use derivative instruments to hedge price risks and this does not necessarily present a high money laundering risk.

➢ Firms should ensure that any factors mitigating the jurisdictional or other risks of a customer are adequately documented and periodically reviewed in the light of international findings or developments, and due diligence gathered as part of ongoing monitoring.

➢ Firms should take a holistic view of the risk associated with a given situation and note that the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

➢ For discussion of other risk areas firms may need to take into account, such as corruption risk, see paragraph 18.20.

18.18 When dealing on an exchange or trading platform, a firm needs to identify its counterparty (section D below describes who should be subject to CDD) and consider any associated risks:

➢ Where there is a CCP, a firm must assess the risks associated with the exchange. For example, what value can be placed on the exchange’s admission procedure, does the exchange carry out due diligence on potential members, can private individuals be members?

➢ If there is no CCP, a firm will need to perform due diligence on the party with whom it deals - even if their name is not known until after the trade - before the trade is settled.

➢ As a result of trading on an exchange or trading platform, a firm may execute a trade with a member who does not have an account with the firm. A firm should consider obtaining, from the exchange or trading platform, a list of members and either identify and verify them upfront (to avoid possible delays in settlement) or on a case by case basis. In some cases platforms operators provide credit management functionality which has the effect of restricting execution of trades to certain counterparties only.

18.19 Product risk should also be considered. Transactions which give rise to cash movements (such as those associated with structured products) may present an increased money laundering risk, although this risk may be mitigated by the nature and status of the customer and the depth of the relationship the customer has with the firm. For example, if the use of a particular product is part of a wider business relationship, and is compatible with other activity between the firm and the customer, the risk may be reduced.

18.20 While assessing ML/TF risks, firms will also wish to assess other factors such as reputational risk, sanctions risks and bribery and corruption risks. For example:

➢ New customers and payments on behalf of clients to third parties will typically need to be screened for sanctions purposes, and new additions to sanctions lists checked against existing clients, in line with the firm's approach to sanctions compliance.
Firms should assess whether they have a due diligence requirement in respect of any introducing brokers who introduce new customers or other intermediaries and consider whether there are any red flags in relation to corruption risks.

D. Customer due diligence, including simplified and enhanced due diligence

Who is the customer?

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

18.22 Where the firm’s customer qualifies for simplified due diligence (see Part I, section 5.4), or is otherwise assessed as posing a lower risk, a lesser extent of CDD may be appropriate (as described by Chapter 5).

18.23 Therefore, from an AML/CTF perspective, as a rule of thumb (although see Part I, Chapter 5, section 5.3.4):

➢ If the firm is acting as principal with another exchange member, the exchange member is the firm’s customer.

➢ As discussed in paragraph 18.18 above, where an exchange-based trade is randomly and automatically matched with an equal and opposite exchange-based trade, it is recognised that, due to market mechanisms, the name of the other exchange member(s) may not be known. In these situations, where all the parties are members of the exchange and there is a CCP to match and settle the trades, the firm cannot know and therefore does not need to identify the other exchange member. Firms should, however, include the money laundering risk involved in the participation in any exchange or centralised clearing, as part of their overall risk-based approach. Participation in any exchange or centralised clearing system does not remove the need to adequately verify its own customer if the firm is dealing as agent for a customer.

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

➢ Where a firm executes a trade OTC with a customer, which is then centrally cleared, and settled by the CCP, the firm has visibility of the customer and may need to verify the identity of the customer with whom they contract. By contrast, the CCP would not be a customer of the firm, and as such the firm would not be required to conduct due diligence on the CCP from an AML/CTF perspective. In certain situations, the firm may open customer accounts at the request of a CCP, in which case due diligence obligations would arise. However, this would only occur in a default management scenario, and such arrangements would be documented in a separate customer agreement with the CCP.

➢ Where a firm is acting as agent for another party, the party for whom the firm is acting will be the firm’s customer.

➢ Where the firm is transacting with a counterparty trading as agent for underlying entities, the counterparty will be the customer of the firm provided simplified due diligence can be applied, or provided that the counterparty is otherwise assessed as posing a lower risk. See Part I, Chapter 5, section 5.6.36ff, which considers whether/when underlying entities will also be customers of the firm.

18.24 Where the firm is performing services on behalf of an investment manager, the investment manager is the firm’s customer. An investment manager may itself be acting on behalf of an underlying entity, such as a fund, to whom it may provide advisory or discretionary investment management services. Whether CDD is performed on the underlying entity will depend on the firm’s business relationship with both entities and the nature and status of the investment manager. As stated in Part I, Chapter 5, paragraph 5.6.38, where a firm takes instruction from
an underlying entity, or where the firm acts on the underlying entity's behalf (e.g., as a custodian), the firm then has an obligation to carry out CDD measures in respect of that entity.

18.25 Accordingly, when determining whether CDD should be performed on the underlying entity, firms may wish to undertake a risk assessment that includes consideration of whether:

(i) the investment manager or the underlying entity is the instructing party (e.g. does the investment adviser/manager have discretionary trading authority and full control to instruct transactions);

(ii) the investment manager is incorporated in a jurisdiction assessed, by the firm, as lower risk;

(iii) the investment manager is subject to and supervised for compliance with satisfactory anti-money laundering requirements, for example because it is subject to national legislation implementing the EU Fourth Money Laundering Directive; and/or

(iv) the product or service is assessed, by the firm, as lower risk (see 18.19 above).

18.26 In circumstances where the firm determines that CDD should be performed on the underlying entity, the firm may consider reliance subject to provisions of Regulation 39 of the ML Regulations (see Part I, Chapter 5, section 5.6.1 – 5.6.23), with regards to CDD on the underlying entity.

18.27 Where a firm is receiving services from a counter-party broker, the firm is the customer of the counter-party broker and it is not required to conduct CDD on that broker (although it may decide, on a risk based approach, that some form of due diligence is appropriate).

Other multi-partite relationships

18.28 An introducing broker may “introduce”, or a Receiver and Transmitter of orders may pass orders from, his customers to a firm to execute trades and, possibly, to perform related requirements in connection with the customers’ trades and bookkeeping and record keeping functions. A fee is paid by the firm to the introducing broker, usually based on the transactions undertaken. A customer often has no say in which firm the introducing broker selects to execute a particular trade. As such, the customer being introduced is a customer of both the introducing broker and the firm. Although an introducing broker may not be considered the firm's customer, a firm may wish to consider whether it should carry out due diligence, in particular in light of the “corporate offences” contained in the Bribery Act 2010 and/or the Criminal Finances Act 2017, as the introducing broker may be considered an “associated person”.

18.29 A non-clearing member of an exchange may maintain one or several accounts with a clearing member. Where a non-clearing member deals as agent for a customer, this may be through an omnibus account with the clearing member on behalf of all the non-clearing member’s underlying customers, who often have no say in the non-clearing member’s selection of a clearing member.

➢ Where a non-clearing member deals on a proprietary basis as principal, it will generally operate a separate account for such business. In that case the non-clearing member will be the customer of the clearing member.

➢ The clearing member may, based upon his risk-based approach and/or the status of the non-clearing member, consider that the non-clearing member’s underlying customer or customers are also his customers. For further guidance refer to Part I, sections 5.3 and 5.4.

18.30 Customers wishing to execute and clear transactions on regulated markets may do so using separate executing and clearing brokers. To complete such a trade, the executing broker will
execute the order and then 'give-up' that transaction to the clearing broker for it to be cleared through the relevant exchange or clearing house.

18.31 This arrangement may commonly take the form of a tri-partite agreement between the customer, the executing broker and the clearing broker. However, give-up arrangements can extend to cover a number of different types of relationships.

18.32 As set out in paragraph 18.63 of this chapter, where a firm acts as executing broker, the party placing the order is the customer for AML/CTF purposes.

18.33 Where a firm acts as clearing broker, the customer on whose behalf the transaction is cleared is the customer for AML/CTF purposes. A clearing broker typically has a more extensive relationship with the customer as they may also act as custodian.

18.34 Where an executing broker and a clearing broker are involved in a 'give up' arrangement, the executing broker may, as part of its risk-based assessment, consider it appropriate to place reliance on the clearing broker (subject to the guidance and requirements within Part I, Chapter 5, paragraphs 5.6.4ff).

18.35 In some cases, other parties, who are not customers under the ML Regulations, may be linked to a transaction. A firm may, however, still wish to assess them as part of its own commercial due diligence and to guard against reputation, sanctions and bribery and corruption risks (e.g., introducing brokers, particularly in higher risk jurisdictions, for the reasons described above).

Distributors

18.36 Firms who use third party distributors to distribute, sell and/or market particular products will generally have a customer relationship with the distributor, rather than the underlying entity (who is the customer of the distributor).

18.37 Firms should carry out CDD on the distributor in accordance with the provisions of Part I and will wish to consider seeking information and/or assurances about the distributor's own AML procedures (and the procedures the distributor has in place to mitigate other financial crime risks). The firm can also seek contractual protections in the distribution agreement.

Introducers of structured products contracting via custodians

18.38 In one scenario, an introducer (who may also be described as an “arranger” or “retrocession agent”) may approach a firm to request, on behalf of an undisclosed client, a quote for a structured product with a particular set of features (e.g., reference assets/indices, capital guarantee, maximum upside, etc). If this quote is acceptable, the introducer will then recommend the structured product to his/her client. The introducer’s client will typically contact their custodian bank to instruct the bank to purchase the structured product from the firm. The custodian bank will purchase, on an execution-only basis, the structured product as principal, settling directly with the firm. The firm then pays the introducer a fee, which is non-standardised and negotiated on a transaction by transaction basis. Alternatively, the firm may approach the introducer with a structured product that the introducer’s clients may be interested in (although transaction flows remain the same as above).

18.39 In some cases, the introducer may act with a power of attorney from their client and thus have authority to purchase the structured product on behalf of the client. The firm should ascertain whether the introducer is acting under a power of attorney or not. Settlement of the transaction will be effected, by the firm, with the custodian bank of the undisclosed client, as outlined above.

18.40 Depending on local legislation, an introducer may or may not be required to be regulated in the country of his domicile or the countries of his/her main operation, which may be different. In Switzerland, for example, introducers who act exclusively in an advisory capacity do not need to be regulated but where the client gives an introducer power of attorney to transact on his behalf with the custodian bank, the introducer has to be regulated for AML purposes, but not conduct of business purposes, with one of the local Self Regulatory Organisations.
18.41 In each of the scenarios outlined above, the introducer should be subject to CDD. As part of that CDD, a firm should check that the introducer satisfies the authorisation requirements (if any) of the introducer’s country of domicile and main countries of operation. The firm should also consider obtaining details of the career in the financial services industry of each of the main employees or principals of the introducer.

In addition, if the custodian bank cannot be subject to simplified due diligence or is not otherwise regarded as posing a lower risk, the firm will also have to look through to the custodian’s underlying customers (the beneficial owners). Firms may also wish to refer to the ‘Retailed Structured Products: Principles for managing the provider-distributor relationship’ guidance, that was published in July 2007 by the European Securitisation Forum (ESF), International Capital Market Association (ICMA), International Swaps and Derivatives Association (ISDA) and the Association for Financial Markets in Europe (AFME). A copy of this guidance is available from the website of any of the above organisations. Firms may also wish to refer to this guidance to assist them in understanding the types of underlying entities that are linked to an individual introducer, together with the particular type of products and tenor of the products that the underlying entities are interested in. Such information may assist firms to understand the expected type and level of business that an introducer may bring to a firm.

18.42 Firms should consider, if an introducer requests that his fee be paid to a bank account held in the name of an apparently unrelated third party or to an account at a bank in a country with no obvious connection to his country of domicile or his countries of main operation, whether such requests give rise to suspicions of bribery, corruption or tax evasion. Firms may wish to consider introducing a policy of paying fees only to a bank account in the name of the introducer that is held at a bank in the country of the introducer’s domicile or a country of main operation. Firms may also wish to confirm that there is full disclosure of any fees on relevant documentation for each transaction.

18.43 Firms should also be alert to the risk that an introducer who is an individual may be carrying on their own personal business whilst still employed by, and managing the affairs of clients of, another firm such as a bank, asset manager or wealth manager. The introducer may be acting in his/her own name or via a corporate which he/she controls. If, as a result of its CDD, a firm has suspicions that an introducer may be currently employed by a financial institution, the firm should contact the financial institution concerned to ascertain whether the individual is employed by them and, if so, that they are content with the proposed relationship between the firm and their employee. Similar suspicions may also arise where all of an introducer’s clients use the same custodian bank.

Expected activity

18.44 A firm will, as part of CDD, assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship and/or transaction. This information will assist firms when assessing whether the proposed relationship is in line with expectations and will support ongoing monitoring. The key consideration is being able to identify whether the client’s activity (for example: transaction size and frequency) is in line with the firm’s knowledge of the client. The firm will, in many cases, be able to infer the client’s expected activity from the nature of the client itself (e.g. regulated financial institutions can generally be expected to trade products consistent with the typical operating model of such an institution).

18.45 Clients will typically have multiple brokers and deal in a multitude of products and asset classes and their strategy may be dependent on market conditions, which may influence changes in activity.

Source of wealth

18.46 A firm should, where appropriate, identify the source of wealth relevant to the business relationship and/or transaction. In the wholesale markets, the source of wealth for a counterparty may often be identifiable from the nature of the customer’s business. Firms may wish to infer source of wealth where the relationship is deemed to be lower risk. However,
where the relationship is with an entity which is indicative of personal wealth of an individual or a collective group of individuals (e.g. family offices), a firm may take additional steps to identify and verify, where appropriate, the client's source of wealth (see also Part II, Chapter 5 on wealth management). Additionally, if settlement or collateral posting is received from a third party, firms should consider the rationale for this.

**Source of funds**

18.47 The source of funds may be identified and verified in certain situations to ensure the origin of the funds involved in the business relationship or occasional transaction is understood. Whether the identification and verification of a customer's source of funds is required will depend on the nature and status of the entity wishing to execute and clear wholesale markets transactions. If the entity is within points (i) and (ii) below (i.e. having an appropriately regulated and supervised status), or is otherwise determined to present a low ML/TF risk, the firm may, on a risk-based approach, conclude that it is not necessary to obtain specific evidence of the source of funds:

(i) subject to requirements in national legislation implementing the EU Fourth Money Laundering Directive (or equivalent) as an obliged entity (within the meaning of that Directive); and

(ii) supervised for compliance with those requirements in accordance with Chapter VI of the EU Fourth Money Laundering Directive (or equivalent).

18.48 In situations where the customer takes the form of a privately-controlled, unregulated entity (including, in particular a private investment company, SPV or family office) the risk is likely to be assessed as higher, and in cases which present a higher ML/TF risk, the source of funds for a business relationship or occasional transaction should be identified and, on a risk-based approach, verified by a firm in order for the firm to reasonably satisfy itself that the origin of the funds is legitimate.

**Simplified due diligence**

18.49 A firm may apply SDD measures in relation to a particular business relationship or transaction if it determines that, taking into account its risk assessment and the matters specified in Regulation 37 of the ML Regulations, the business relationship or transaction presents a low degree of risk of ML/TF.

18.50 In the wholesale markets, a firm will often interact with other regulated firms, some of whom may be acting on behalf of underlying entities. In this context, firms should have regard to paragraphs 18.23 to 18.27 of this Chapter.

**Enhanced due diligence (including Correspondent Relationships)**

18.51 The ML Regulations prescribe that EDD measures are required to be carried out in respect of Correspondent Relationships with Respondents based in non-EEA jurisdictions (see Part II, Chapter 16 for the definition of a “Correspondent Relationship”).

- For respondents based in EEA member states, the firm's risk assessment will require EDD measures to be applied if the firm determines that the relationship presents a higher degree of ML/TF risk.

18.52 Otherwise, product risk alone will not ordinarily be the determining factor in a firm assessing whether an enhanced level of due diligence is appropriate; therefore there are no enhanced due diligence requirements specific to the wholesale markets sector, over and above those set out in Part I, section 5.5, which take into account other risk factors such as client type and jurisdictional risk.
E. Monitoring and surveillance

18.53 Guidance on general monitoring requirements is set out in Part I, section 5.7.

18.54 Monitoring in wholesale firms will be affected by the fact that firms may only have access to a part of the overall picture of their customer’s trading activities. The fact that many customers spread their activities over a number of financial firms will mean that many firms will have a limited view of the entirety of a customer’s trading activities. Extreme market conditions may also impact on a customer’s trading strategy and the commercial rationale for a particular transaction will often be linked to market conditions. There are, however, specific characteristics of the wholesale market sector which will impact a firm involved in the wholesale markets monitoring activity. These include:

➢ Scale of activity: The wholesale markets involve very high volumes of transactions being executed by large numbers of customers. The monitoring activity undertaken should therefore be adequate to handle the volumes undertaken by the firm.

➢ Use of multiple brokers: Customers may choose to split execution and clearing services between different firms and many customers may use more than one execution broker on the same market. The customer’s reasons for this include ensuring that they obtain best execution, competitive rates, or to gain access to a particular specialism within one firm. This will restrict a firm’s ability to monitor a customer, as they may not be aware of all activity or even contingent activity associated with the transactions they are undertaking.

➢ Electronic execution: There is an increasing use of electronic order routing where customers access markets directly and there is little or no personal contact between the firm and the customer in the day-to-day execution of the customer’s business. This means that the rationale for particular transactions may not be known by the firm.

18.55 The nature and extent of any monitoring activity will therefore need to be determined by a firm based on an assessment of its particular business profile. This will be different for each firm and may include an assessment of the following matters:

➢ extent of execution vs clearing business undertaken;
➢ nature of customer base (geographic location, regulated or unregulated);
➢ number of customers and volume of transactions;
➢ types of products traded and complexity of those products; and/or
➢ payment processes (including payments to third parties, if permitted).

18.56 Firms should ensure that any relevant factors are taken into account in determining their monitoring activities, and that the programme is adequately documented and subject to periodic review on an ongoing basis. Given the bespoke nature of some wholesale market products and the difficulties in developing meaningful rules for electronic monitoring (e.g., a lack of typologies for the sector), it may well be appropriate for a firm to monitor manually. Firms should, however, be able to demonstrate the rationale for their monitoring strategy.

18.57 Firms relying on third parties under the ML Regulations to apply CDD measures cannot rely on the third party in respect of monitoring of transactions and the customer relationship.

18.58 Firms may wish to leverage existing surveillance frameworks established for the purposes of compliance with the Market Abuse Regulation (MAR)\(^2\), to assist in monitoring certain wholesale markets activities for unusual transactions which may constitute financial crime. Where suspicious trading activity is identified and the firm considers it necessary to file a suspicious transaction & order report (STOR), the firm should consider whether the filing of a suspicious activity report (SAR) under the Proceeds of Crime Act (POCA) is also appropriate.

---

\(^2\) [https://www.fca.org.uk/markets/market-abuse](https://www.fca.org.uk/markets/market-abuse)
F. Guidance on specific products

Securities

Product specific risks

18.59 Securities are typically regarded as a lower risk asset class and are a typical product traded on the wholesale markets. Firms should, however, be alive to the risk of insider dealing and market abuse (and the subsequent laundering of the proceeds of such offences) in the context of securities trading.

Who is and is not the customer?

18.60 Customers wishing to transact securities on a DVP basis may do so through an executing broker that will generally settle with the customer’s settlement agent/custodian. Under this arrangement, the customer elects to execute transactions through an executing broker and to clear the transaction through a separate settlement agent/custodian. The orders can either be placed directly by the customer or by an agent on behalf of the customer. Once the transaction is executed, the executing broker will settle with the settlement agent/custodian simultaneously once payment is received.

18.61 Both the executing broker and the settlement agent/custodian will have a relationship with the customer.

18.62 It is usually (but not always) the customer that elects to execute transactions through one or more brokers and to clear such transactions through a settlement agent/custodian and, to that end, selects both parties.

18.63 Where a firm acts as executing broker, the party placing the order is the customer for AML/CTF purposes. Where the party placing the order is acting as agent for underlying entities, they, too, may be customers for AML/CTF purposes. In this context, firms should have regard to paragraphs 18.23 to 18.27 of this chapter.

18.64 Where a firm acts as settlement agent/custodian, the customer on whose behalf the transaction is executed is the customer for AML/CTF purposes.

18.65 A common additional participant in a DVP arrangement is the customer’s investment adviser or manager, to whom the customer has granted discretionary trading authority. Where a firm is acting as executing broker and there is an investment adviser or manager acting for an underlying entity, the CDD performed, and whether there is an obligation to identify the underlying entity, will depend upon the regulatory status and location of the adviser or manager. When considering whether it is necessary to undertake CDD on the underlying entity, firms should have regard to paragraphs 18.25 and 18.26 of this chapter.

Customer due diligence

18.66 Where the underlying entity is to be considered to be subject to CDD by the executing broker, a risk based approach to CDD can take into account the investment manager and/or the settlement agent/custodian’s equivalent regulatory status, pursuant to Part I, paragraph 5.6.4. This may reduce the identity information or evidence requested and what the firm verifies. Firms should take the relationship with the Investment Manager and settlement agent/custodian into account in their own CDD on customers, rather than place full reliance on the settlement agent/custodian.

18.67 Given the information asymmetries likely to exist between an executing broker and settlement agent/custodian, when a firm is acting as settlement agent/custodian it would not be appropriate, from a risk-based perspective, to rely on an executing broker, even if this would be permitted under the ML Regulations. Settlement agents/custodians should undertake the CDD measures as set out in Part I, Chapter 5.

18.68 Where transactions are settled on a free of payment basis, firms should ensure that they understand the commercial rationale for this arrangement.
Monitoring

18.69 See the general guidance on monitoring at section E above.

Money market instruments

Product specific risks

18.70 “Money Market Instruments” is the term used to collectively cover foreign exchange (FX), interest rate products and term deposits. These instruments will typically be traded in the wholesale market between regulated financial institutions and large corporates (listed and private) and the money laundering risk may therefore be viewed as generally lower. However, this risk may be increased by matters such as:

- the nature of the customer (e.g. the customer's business);
- the customer's regulatory status (e.g. a sophisticated private investor);
- the purpose of the trading (e.g. hedging may be regarded as lower risk than speculative transactions);
- requests for payments to be made to third parties: for example, customers, particularly corporates, that need to make FX payments to suppliers and overseas affiliates.

18.71 When assessing the money laundering risk in such circumstances, a firm may want to take into account the nature of the customer’s business and the frequency and type of third party payments that are likely to result from such business.

Who is and is not the customer?

18.72 See the general guidance in paragraphs 18.21 to 18.43.

Customer due diligence

18.73 FX (as well as many other traded products) is commonly traded on electronic trading systems. Such systems may be set up by brokers or independent providers. When a firm executes a transaction on these systems the counterparty’s identity is not usually known until the transaction is executed. The counterparty could be any one of the members who have signed up to the system. Firms should examine the admission policy of the platform before signing up to the system, to ensure that the platform only admits regulated financial institutions as members, or that the rules of the electronic trading system mean that all members are subject to satisfactory anti-money laundering checks, and identify its counterparty and any associated risks (see paragraph 18.18).

Monitoring

18.74 See section E for general guidance on monitoring.

Financial derivatives

Product specific risks

18.75 Financial products are utilised for a wide range of reasons, and market participants can be located anywhere within the world; firms will need to consider these issues when developing an appropriate and holistic risk-based approach. The nature, volume and frequency of trading, and whether these make sense in the context of the customer’s and firm’s corporate and financial status, will be key relevant factors that a firm will need to consider when developing an appropriate risk-based approach. Firms should also consider whether the particular derivative to be traded is consistent with its understanding of the customer's expected activity.

18.76 Where firms are trading commodity futures, they should be mindful of the fact that physical delivery may be required.

18.77 The risks between exchange-traded derivatives and OTC derivative products in the financial derivative markets are the same as those set out in paragraphs 18.10 to 18.15.
18.78 Some derivative products may be complex in nature and linked to a chain of underlying assets. On this basis, where the firm is facilitating the trade of a derivative product, it is not expected to have sight of the specific asset underlying the derivative.

Who is and is not the customer?

18.79 See the general guidance in paragraphs 18.21 to 18.43.

Customer due diligence

18.80 See the general guidance in section D.

Monitoring

18.81 See the general guidance in section E.

18.82 When assessing alerts triggered by a firm's surveillance or other monitoring procedures, firms may wish to consider the nature of the client, and whether the observed activity is consistent with the firm's understanding of that client's expected activity (see also paragraphs 18.44 to 18.45 on expected activity more generally).

Commodities

Product specific risks

18.83 Regulated firms that, in addition to physical commodity activity, undertake any business with a customer which amounts to a regulated activity (including business associated with physical commodities) will be subject to the ML Regulations, including being required to conduct CDD on the customer.

18.84 When implementing a risk-based approach and producing or reviewing risk assessments or the risk profile of a prospective customer, there are a number of areas which commodity market firms may want to take into account in addition to the more general matters set out in Part I, Chapters 4 and 5. These will include, but not be limited to:

➢ The wide range of different business interests which populate the commodity markets. The types of participants may typically include:
  • Producers (e.g. oil producers and mining firms);
  • Users (e.g. refiners and smelters);
  • Wholesalers (e.g. utility firms);
  • Commercial merchants, traders and agents; and
  • Financial firms (e.g. banks and funds).

➢ These types of firm are illustrative and widely drawn and firms can be present in more than one category (for example, a refiner will be both a user of crude oil and a producer of oil products).

➢ The instruments traded in the wholesale commodity markets can allow for the speculative trading, hedging and physical delivery of commodities.

➢ There may be third party funding of transactions in the commodities markets. Also, where a bank is sending funds to a customer to purchase a physical commodity and the customer hedges the risks associated with the transaction in the derivatives market through a broker, the bank may guarantee the payment of margin to that broker; this results in a flow of money between the broker and the bank on the customer's behalf. However, both the party making the payment on behalf of the customer, and the party receiving the funds, will be regulated financial institutions.

➢ Firms should also consider whether it is necessary to assess the potential higher risk of corruption, money laundering, fraud or sanctions issues associated with extractive industries or governmental licences in higher risk jurisdictions through its CDD processes.
The risks and potential mitigating factors should be taken in the round. The global nature of the commodity markets means that firms from potentially higher risk jurisdictions with a perceived higher money laundering risk are likely to have legitimate commercial interests. Understanding the role of a prospective customer in the market, and their reasons for trading, will help inform decisions on the risk profile they present (see paragraph 18.17).

When undertaking commodities business, firms should have particular regard to the sanctions guidance in Part III, to the guidance on financial sanctions produced by the Office of Financial Sanctions Implementation within HM Treasury\(^24\), and to any relevant trade sanctions\(^25\).

Based on the commodities being traded and jurisdictions involved, a firm may consider its obligations under its own policy statement pursuant to the Modern Slavery Act (2015)\(^26\).

Who is and is not the customer?

Where business does not fall within the scope of the ML Regulations, e.g., shipping and chartering, it is entirely a matter for firms to decide what commercial due diligence they perform on their counterparties, and what due diligence they may wish to undertake to mitigate ML/TF and other financial crime risks (e.g. for the purposes of complying with applicable sanctions regimes).

Customer due diligence

See the general guidance at section D.

Monitoring

See the general guidance in section E. Firms should remain alert to the need to carry out sanctions screening (including screening the names of vessels etc.) as part of their ongoing monitoring in this area.

Structured products

Product specific risks

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).

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

- Corporates;
- Private banks;
- Government agencies; and
- Financial institutions.

The money laundering risk associated with structured products is not generally considered to be high, because of the involvement of regulated parties and because trading in structured products is unlikely to be a particularly effective way to launder criminal proceeds. However, because of the sometimes complex nature of the products, they may generally be more difficult to value than cash securities. This complexity may make it easier for money launderers, for example, to disguise the true value of their investments. Firms should therefore remain mindful

---


of their obligations when trading in structured products, and ensure that they carry out EDD where red flags are identified.

18.95 The complexity of the structure can also obscure the actual cash flows in the transaction, enabling customers to carry out circular transactions. Understanding the reason behind a customer’s request for a particular product will help firms to assess the money laundering risk inherent in the structure.

Who is and is not the customer?

18.96 Transactions are normally undertaken on a principal basis between the provider (normally a financial institution) and the customer. Some structured products are also sold through banks and third party distributors (introducers). In the latter circumstances, it is important to clarify where the customer relationships and responsibilities lie (e.g. are the third parties introducing clients to the firm or distributing products on behalf of the firm) and to set out each party’s responsibilities in relation to AML. Where a firm wishes to contract out its customer identification and verification obligation to a distributor, it should establish whose procedures are to be used (e.g. the firm’s or the distributor’s), satisfy the reliance requirements and establish monitoring procedures.

Customer due diligence

18.97 See general guidance on CDD in section D.

Monitoring

18.98 See general guidance on monitoring in section E.