1: Retail banking

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

Overview of the sector

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

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

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

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

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

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

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

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

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

Other relevant industry and regulatory guidance

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

- See "Fighting Financial Crime" pages on www.fsa.gov.uk
- "International Students – opening a UK bank account" and "Banking for people who lack capacity to make decisions" – see www.bba.org.uk

1.10 See also paragraphs 1.38 – 1.41 on financial exclusion.

Customer due diligence

General

1.11 The AML/CTF checks carried out at account opening are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals opening accounts or obtaining services from banks. Firms should 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, the additional precautions required under the 'enhanced due diligence' provisions of the ML Regulations as set out in paragraphs 5.5.10 – 5.5.17. See also 1.35 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 The other documents cited in Part I, paragraph 5.3.74 may be used for UK residents where the standard documents are not available, whether singly or in conjunction, according to the principles set out in that paragraph. For non-UK residents, or persons who have recently entered the UK, firms may well require additional documentary evidence - not for AML/CTF purposes, but to offset fraud and credit risks which would normally be addressed through electronic checks for UK residents (see paragraphs 1.22-1.24).

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

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

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

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

A customer with an existing account at the same firm

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

1.19 Most large firms have completed current customer review (CCR) checks. These could result in different levels of confidence in the identity of the person concerned, depending on the amount of information held on the existing holder. If the review had verified the customer's identity at least to the standard required as part of the CCR exercise, a second account would normally be opened without further identification procedures, (provided the characteristics of the new account are not in a higher risk category than the existing account). Thus, a foreign currency account might require further identification procedures and/or additional customer enquiries but for a new savings account, where the applicant's existing account had passed current customer review checks, most firms would not require further identification.

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

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

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

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

1.22 A non-resident, whether a non-UK national or a UK national who is returning to the UK after a considerable absence, who is physically present in the UK and who wishes to open an account should normally be able to provide standard identification documentation to open a Basic Bank Account (see Part I, paragraph 5.3.74 and Annex 1-I).

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

1.23 Non-residents not physically present in the UK wishing to open an account in the UK are unlikely to wish to open a Basic Bank Account, with its limited facilities. The customer should be able to demonstrate a need for a bank account in the UK, or should fall within the firm's criteria for wealth management clients, in which case the guidance in sector 5: *Wealth Management* will apply. Enhanced due diligence will apply where the customer is not met personally or where other high risk factors come into play (see paragraphs 5.19-24 and Part I, section 5.5).

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

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

Lending

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

1.26 Firms should refer to the guidance on situations where customers are subject to identification by two or more financial services firms in relation to the same transaction, set out in Part I, section 5.6.

Business Banking

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

1.28 Essentially, as set out in Part I, Chapter 5, identification should initially focus on ascertaining information about the business and its activities and verifying beneficial owners holding or controlling directly or indirectly, 25% or more of the shares or voting rights, and controllers, and where the business is a limited company, verifying the legal existence of the company.

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

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

of proposed activities, anticipated cash flow through the accounts, frequency and nature of transactional activity, an understanding of the underlying ownership of the business) and personal identification of the owners/controllers of the business, as well as information on their previous history. Part I, Chapter 5, contains further guidance relating to identification standards.

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

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

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

1.34 In determining the identification appropriate for partnerships (see Part I, paragraphs 5.3.163 - 5.3.177), whose structure and business may vary considerably, and will include professional firms e.g. solicitors, accountants, as well as less regulated businesses, it will be important to ascertain where control of the business lies, and to take account of the risk inherent in the nature of the business.

Enhanced due diligence

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

- When the applicant is a PEP. See Part I, paragraphs 5.5.18 - 5.5.30.
- When there is no face-to-face contact with the applicant. An additional check is needed to offset the increased risk, notably that of impersonation fraud (see Part I, paragraph 5.3.82).
- When the business of the customer is considered to present a higher risk of money laundering or terrorist financing. Examples should be set out in the firm's risk-based approach and should reflect the firm's own experience and information produced by the authorities. See Part I, paragraphs 3.24 – 3.26 and section 5.5 for general guidance.
- When establishing a correspondent banking relationship with an institution in a non-EEA state, (although in practice most firms would not regard such relationships as forming part of their 'retail' business).

1.36 Firms will need to consider making more penetrating initial enquiries, over and above that usually carried out before taking on businesses whose turnover is likely to exceed certain thresholds, or where the nature of the business is higher risk, or involves large cash transactions,

or is conducted primarily on a non face-to-face basis. Recognising that there are a very large number of small businesses which are cash businesses, there will be constraints on the practicality of such enquiries; even so, firms should be alert to the increased vulnerability of such customers to laundering activity when evaluating whether particular transactions are suspicious. Examples of higher risk situations are:

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

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

Financial exclusion

1.38 Denying those who are financially excluded from access to the financial sector is an issue for deposit takers. Reference should be made to the guidance given in Part I, paragraphs 5.3.110 to 5.3.114, and Annex 1-I.

1.39 The "financially excluded" are not a homogeneous category of uniform risk. Some financially excluded persons may represent a higher risk of money laundering regardless of whether they provide standard or non standard tokens to confirm their identity, e.g., a passport holder who qualifies only for a basic account on credit grounds. Firms may wish to consider whether any additional customer information, or monitoring of the size and expected volume of transactions, would be useful in respect of some financially excluded categories, based on the firm's own experience of their operation.

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

1.41 Where an applicant produces non-standard documentation, staff should be discouraged from citing the ML Regulations as an excuse for not opening an account before giving proper consideration to the evidence available, referring up the line for advice as necessary. It may be that at the conclusion of that process a considered judgement may properly be made that the evidence available does not provide a sufficient level of confidence that the applicant is who he claims to be, in which event a decision not to open the account would be fully justified. Staff should bear in mind that the ML Regulations are not explicit as to what is and is not acceptable evidence of identity.

Monitoring

1.42 Firms should note the guidance contained in Part I, section 5.7, and the examples of higher risk businesses in paragraph 1.36. It is likely that in significant retail banking operations, some form of automated monitoring of customer transactions and activity will be required. However, staff vigilance is also essential, in order to identify counter transactions in particular that may represent money laundering, and in order to ensure prompt reporting of initial suspicions, and application for consent where this is required.

1.43 Particular activities that should trigger further enquiry include lump sum repayments outside the agreed repayment pattern, and early repayment of a loan, particularly where this attracts an early redemption penalty.

1.44 Mortgage products linked to current accounts do not have a predictable account turnover, and effective rescheduling of the borrowing – which can be repaid and re-borrowed at the borrower's initiative – does not require the agreement of the lender. This should lead to the activity on such accounts being more closely monitored.

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

Training

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

Reporting

1.47 Firms should note the guidance contained in Part I, Chapter 6. As indicated in Part I, paragraphs 7.31 to 7.33, further reference material and typologies are available from the external sources cited, viz: JMLSG, FATF and SOCA websites. In addition, firms should be aware of the requirement under Section 331(4) of the Proceeds of Crime Act for reports to be submitted "as soon as practicable" to SOCA.

1.48 There is no formal definition of what "as soon as practicable" means, but firms should note the enforcement action taken by the FSA in respect of the anti money laundering procedures in place at a large UK firm. The FSA imposed a financial penalty on the firm due, in part, to finding that over half of the firm's suspicious activity reports were submitted to SOCA more than 30 days after having been reported internally to the firm's nominated officer. In view of the volumes of reports which may be generated in this sector, firms may wish to keep under review whether their nominated officer function is adequately resourced. 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 SOCA. In all circumstances, however, firms should ensure that their end to end process is as efficient as it can be.

Interbank Agency Service

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

ANNEX 1-I

Special Cases

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

Customer	Document(s)
Benefit claimants	Entitlement letter issued by DWP, HMRC or local authority, or Identity Confirmation Letter issued by DWP or local authority
Those in care homes/sheltered accommodation/refuge	Letter from care home manager/warden of sheltered accommodation or refuge Homeless persons who cannot provide standard identification documentation are likely to be in a particular socially excluded category. A letter from the warden of a homeless shelter, or from an employer if the customer is in work, will normally be sufficient evidence.
Those on probation	It may be possible to apply standard identification procedures. Otherwise, a letter from the customer's probation officer, or a hostel manager, would normally be sufficient.
International students	Passport or EEA National Identity Card AND Letter of Acceptance or Letter of Introduction from Institution on the UK Border Agency list (see http://www.bia.homeoffice.gov.uk/employers/points/sponsoringmigrants/registerofsponsors/. See the pro forma agreed for this purpose with UKCOSA: The Council for International Education, attached as Annex 1-II. See also Part I, paragraphs 5.3.107-108.
Prisoners	It may be possible to apply standard identification procedures. Otherwise, a letter from the governor of the prison, or, if the applicant has been released, from a police or probation officer or hostel manager would normally be sufficient. See the pro forma agreed for this purpose with the National Offender Management Service and UNLOCK, attached as Annex 1-III
Economic migrants *[here meaning those working temporarily in the*	National Passport, or National Identity Card (nationals of EEA and

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

Notes:

1. Passports, national identity cards and travel documents must be current, i.e. unexpired. Letters should be of recent date, or, in the case of students, the course dates stated in the Letter of Acceptance should reasonably correspond with the date of the account application to the bank. All documents must be originals. In case of need, consideration should be given to verifying the authenticity of the document with its issuer.

2. As with all retail customers, firms should take reasonable care to check that documents offered are genuine (not obviously forged), and where these incorporate photographs, that these correspond to the presenter.

3. Whilst it is open to firms to impose additional verification requirements if they deem necessary under their risk based approach and to address the perceived commercial risks attaching to their own Basic Account products, they should not lose sight of the requirement under *SYSC 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."

ANNEX 1-II

(To be typed on education institution letterhead)

LETTER OF INTRODUCTION FOR UK BANKING FACILITIES

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

Course Details

Name of Course:

Type of Course:

Start Date:

Finish Date:

Address Details [if known]

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

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

The Student's UK Address is: [if known]
(Please insert the Student's UK Address)
……
……
……
……

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

Signed…….

Name……..…

Position……...

Contact Telephone Number at education institution……..

ANNEX I-III

Ministry of JUSTICE
National Offender Management Service

PERSONAL IDENTIFICATION DOCUMENT

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

Name…….

Nationality ……. Place of Birth……..

Signature..…… Date……..

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

…….

…….

Witnessed by

…….

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

…….

Signature of witness

…….

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 ……Position ……..……

e-mail address ……@hmps.gsi.gov.uk

Direct telephone line ……

Signature …… Date …….