4: Credit unions

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

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

Overview of the sector

4.1. The membership of a credit union is restricted to individuals who fulfil a specific qualification which is appropriate to a credit union (and as a consequence a common bond exists between members) - Credit Unions Act 1979, s1(2)(b). The common bond concept is central to the co-operative ethos of a credit union and is also fundamental to the regulatory regime for credit unions.

4.2. The FCA has produced additional common bond guidance outlining acceptable forms of common bond according to legislation.

4.3. Credit unions therefore operate within a restricted, often localised market, providing services to members, not to the public at large, which results in potentially lower risks.

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

4.4. The majority of credit unions offer very basic savings and loan products, although some offer more flexibility around the products they can provide. Overall, however, credit unions are restricted in terms of the range and complexity of the products they can offer and to whom they can offer them.

4.5. There are limits on the level of savings a credit union can hold on behalf of an individual member, which are set out in Section 2 of the Credit Union Part, PRA Rulebook. The return on savings is typically paid as a dividend linked to financial performance. In addition, there are rules governing a credit union's lending activity. Lending limits are set out in CREDS 7.2 and Section 3 of the Credit Union Part, PRA Rulebook.

4.6. Credit union deposits are often collected from payroll deductions, benefit deductions, or regular standing orders from a designated bank account. Withdrawals are managed via a single nominated current account. Transactions from unknown third parties are relatively uncommon, thus reducing the money laundering and terrorist financing risks.

4.7. Therefore credit union financial products do not deliver sufficient functionality or flexibility to be the first choice for money launderers, although these restrictions may not be such a deterrent to terrorist financiers.

4.8. For some credit unions, the high levels of cash transactions going through some credit union accounts may be one area where there is a higher risk of money laundering or terrorist financing,

e.g., by 'smurfing'[1], although credit unions are moving away from high transaction volume, cash-based business models.

4.9. The number of staff and volunteers involved in the day to day operations of a credit union is relatively small and, even in larger credit unions, there are typically no more than a few individuals whose responsibility it is to manually process data. Therefore, where there is manual processing of all transactions, the ability to identify suspicious transactions is potentially much greater. In addition, the relatively small organisational structures mean that suspected money laundering or terrorist financing can be detected and reported much faster in smaller credit unions than it could in other financial services firms. The monitoring procedures for larger credit unions, that inevitably do not have such a close relationship with their members, will need to reflect the absence of those relationships, to ensure that potential problems, e.g., 'smurfing', can be detected.

4.10. This does not, of course, mean that there is no risk of money laundering or terrorist financing in credit unions and credit unions must in any case be aware of their responsibilities under the ML Regulations, the Proceeds of Crime Act (POCA) and the Terrorism Act. Credit unions must therefore establish appropriate procedures to monitor activities, with a particular scrutiny of those that carry a higher risk of money laundering or terrorist financing (see Part I, section 5.7). Examples of such activities include:

- money transfers to third parties;
- large one off transactions;
- third parties paying in cash on behalf of the member;
- unusual loan or saving transactions;
- reluctance to provide documentary evidence of identity when opening an account (even when taking into account financial exclusion issues).

Applying a risk-based approach

4.11. In accordance with the guidance in Part I, Chapter 4, a credit union's risk-based approach will ensure that its strategies are focused on deterring, detecting and disclosing in the areas of greatest perceived vulnerability. The credit union needs to take a number of steps, documented in a formal policy statement which assesses the most effectual, cost effective and proportionate way to manage money laundering and terrorist financing risks. These steps are:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the credit union's particular
  - Members;
  - Products;
  - Delivery channels;
  - Geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done and why.

Steps taken by a credit union will include identifying politically exposed persons (PEPs) by introducing systems and controls which are in line with the nature and size of the credit unions, using information gathered by the credit union during the onboarding process. This may involve using information reasonably available to them, including a variety of public domain information (such as parliamentary and government websites, reliable news sources and public registers), but the use of commercial databases is not mandatory.

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

4.12. A credit union will need to take account of its own experience and knowledge of its members and their financial activities. Credit unions should also consult the Financial Action Task Force website at www.fatf-gafi.org in order to keep up-to-date with money laundering/terrorist financing typologies.

4.13. Following the establishment of a risk-based approach, it is the responsibility of the credit union's senior management to keep this strategy under regular review. Credit unions may consider it appropriate to have a standing item covering money laundering on the agenda of their monthly meeting to ensure procedures are being regularly reviewed. Credit unions will also need to take into account SYSC 6.3.8 which reads, "a firm must allocate to a director or senior manager (who may also be the money laundering reporting officer) overall responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls".

Customer due diligence

4.14. The anti-money laundering (AML)/combating the financing of terrorism (CTF) checks carried out during account opening are one of the primary controls for preventing criminals opening an account and are therefore an important element of AML/CTF procedures. Credit unions should be satisfied that the policies and procedures in place for verifying identity are effective in preventing and detecting money launderers and that they make provision for circumstances when increased evidence is required.

4.15. For the majority of members, the standard identification requirement set out in Part I, Chapter 5 (full name, residential address and date of birth) including, in the case of customers not met face to face, consideration of the additional precautions set out in Part I, paragraphs 5.3.85 – 5.3.90. Where relevant, obtaining the additional customer information set out in Part I, section 5.5, will be applicable.

4.16. The identity information should be verified in accordance with the guidance set out in Part I (paragraphs 5.3.72-5.3.84), either from documents produced by the individual, or electronically, or through a combination of the two: these approaches are potentially equal options, depending on the circumstances in any given case.

Documentary verification

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

Electronic verification

4.18. Electronic verification may be used to meet a firm's customer identification obligations. However, a credit union should first consider whether electronic verification is suitable for its membership base, and should then have regard to the guidance in Part I, paragraphs 5.3.52-5.3.53 and 5.3.79–5.3.84. When using electronically-sourced evidence to verify identity, credit unions should ensure that they have an adequate understanding of the data sources relied on by

the external agencies that supply the evidence. Credit unions should be satisfied that these sources provide enough cumulative evidence to provide reasonable certainty of a person's identity, and conform with the guidance set out in Part I, Chapter 5. An electronic check that accesses a single database (e.g., Electoral Register check) is normally not enough on its own to verify identity.

Financial exclusion

4.19. The FCA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. The term is sometimes used in a narrower sense; for example, the Financial Inclusion Commission refers to those who, for specific reasons, do not have access to mainstream banking or financial services – that is, those at the lower end of income distribution who are socially/financially disadvantaged and in receipt of benefits, or those who chose not to seek access to financial products because they believe that they will be refused.

4.20. As a first step, before concluding that a member cannot produce evidence of identity, credit unions will have established that the guidance on initial identity checks for personal customers set out in Part I, paragraphs 5.3.72-5.3.84 cannot reasonably be applied. Where the credit union has concluded that a member cannot reasonably be expected to meet the standard identification requirements, the guidance in Part I, paragraphs 5.3.115–5.3.116 should be followed. Where the alternative evidence set out in sector 1: *Retail banking*, Annex 1-I cannot be applied, a letter or statement from an appropriate person[2] who knows the individual, that indicates that the person is who he says he is, can be accepted as evidence of identity.

4.21. Where a credit union has concluded that it should treat a member as financially excluded, a record should be kept of the reasons for doing so.

Employee credit unions

4.22. Roughly ten percent of British credit unions are employee credit unions, but they represent a significant proportion of the overall assets and membership of the movement. All members of employee credit unions share the common bond of being associated with one particular employer or employer group, which must be large enough to provide enough members to sustain a viable credit union. The most common examples of employee credit unions are local authority, police and transport credit unions.

4.23. Employee credit unions should also have their own standard identity verification requirements to ensure that the member is indeed an employee (e.g., wage slip, employee identity card, other documented knowledge that the credit union has) and have therefore undertaken the appropriate identity checks. It should be noted that these checks are for the purpose of satisfying the common bond qualification for membership, as opposed to being for AML/CTF purposes.

4.24. To satisfy the requirements of AML/CTF legislation, additional identity verification checks should be sought, as described in paragraphs 4.15–4.17 of this chapter.

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

4.25. Employee credit unions whose common bond extends to family members of employees should seek the standard verification information from each family member. In these circumstances credit unions should follow the guidance in Part I, paragraphs 5.3.72–5.3.116.

Live or work credit unions

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

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

Credit union activity in schools

4.28. Many credit unions have established links with their local schools. For many credit unions, establishing partnerships with local schools is a key part of their long-term development strategy. Under a risk-based approach in terms of membership profile and level of activity undertaken by junior savers, credit unions can reasonably assume that children saving in a savings club set up through a school present a lower risk of the credit union being used for money laundering purposes. **Credit Unions must, however, monitor the junior accounts, inter alia to ensure that adults are not laundering through the account.**

4.29. Where any potential member cannot reasonably be expected to produce detailed evidence of identity, it should not be a consequence that they are denied access to financial services. If a credit union decides that a particular child cannot reasonably be expected to produce such evidence, the reasons for adopting the 'financial exclusion' approach should be clearly documented. In relation to a schoolchild, a credit union should follow the guidance in Part I, paragraphs 5.3.118 and 5.3.120. In cases where standard identification evidence is not available, it may accept a letter or statement from an appropriate person as evidence of identity. In such cases, a letter from the school should include the date of birth and permanent address of the pupil on the school's letter headed paper to complete standard account opening procedures.

4.30. In cases where there is an adult signatory to the account and the adult has not previously been identified to the relevant standards because they do not already have an established relationship with the credit union, the identity of that adult must be verified, in addition to the identity of the child, see Part I, paragraph 5.3.120.

Junior Savers

4.31. In addition to offering a credit union service to minors through schools' clubs, many credit unions offer children a savings facility direct with the credit union. In such cases, credit unions should seek identification evidence as set out in Part I, paragraphs 5.3.118–5.3.120. Where standard identification cannot be produced for the child, other evidence such as a letter from the school which includes the date of birth and permanent address of the pupil on the school's letter headed paper, should be sought to complete standard account opening procedures.

4.32. Often, the junior account will be established by a family member or guardian. In cases where the adult opening the account has not previously been identified to the relevant standards because they do not already have an established relationship with the credit union, the identity of that adult must be verified, in addition to the identity of the child, see Part I, paragraph 5.3.120.

Enhanced due diligence

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

- when the person is involved in a business that is determined to present a high risk of money laundering; examples of high risk businesses can be found in paragraphs 1.36-1.38 of sector 1: *Retail banking*
- When the proposed customer relationship or transaction is with a person established in a high risk non-EEA country;
- where the customer is a PEP, or a family member or close associate of a PEP
- Where a customer has provided false or stolen identification documentation or information on establishing a relationship;

Additional customer information

4.34. Credit unions will need to hold sufficient information about the circumstances of members in order to monitor their activity and transactions. Therefore 'Knowing Your Customer' is about building a relationship with the membership and knowing when to ask the appropriate questions at the appropriate time. Reasonable enquiries of a member, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of knowing the customer and monitoring, and should not give rise to tipping off. Although not a prescriptive list, examples of when additional customer information is needed include: a change in circumstances (name, address, employer), a lump sum payment or a change in transaction behaviour. Credit unions may detect significant changes in circumstances when for example, carrying out a loan application, which may require the credit union to seek further information, and to update member profiles which are used as the basis of monitoring customer transactions.

4.35. Credit unions must also obtain information about the nature and purpose of the relationship with the member. In the majority of cases, this may be obvious from the service provided, but the credit union may also be providing loans to sole traders for business purposes and information on such relationships must be obtained.

4.36. The extent of information sought and of the monitoring carried out in respect of any particular member will depend on the money laundering and terrorist financing risk that they present to the credit union. Credit unions should also have regard to the guidance in Part I, section 5.5.

Monitoring customer activity

4.37. As mentioned in paragraphs 4.8-4.9, credit unions must establish a process for monitoring member transactions and activities which will highlight unusual transactions and those which need further investigation. It is important that appropriate account is taken of the frequency, volume and size of transactions. Although not a prescriptive list, an example of a simple approach for credit unions that deal mainly in small sum transactions may be: to investigate deposits over a certain amount, frequency of members' deposits and members whose deposits may appear erratic. However, for larger credit unions that have more complex operational structures, a more sophisticated approach may be needed, e.g., asking who is making deposits in relation to a junior account.

4.38. The key elements to monitoring are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and to ask pertinent questions to elicit the reasons for unusual transactions.

4.39. Also key to a successful monitoring process is staff and volunteer alertness (see Part I, Chapter 7).

4.40. Credit unions must be aware that unusual does not always mean suspicious and therefore should not be the routine basis for making reports to the NCA. Identifying what is unusual is only the starting point – firms need to assess whether what is unusual gives rise to suspicion and report accordingly.

Reporting

4.41. General guidance on reporting is given in Part I, Chapter 6. All staff and volunteers need to know the identity of the nominated officer, so that they know to whom to report suspicious activity.

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

Training

4.43. General guidance on staff awareness, training and alertness is given in Part I, Chapter 7. In particular:

- Staff must be made aware of the risks of money laundering and terrorist financing, the relevant legislation and their obligations under that legislation
- Staff must be made aware of the identity and responsibilities of the firm's nominated officer and MLRO
- Staff must be trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions
- Staff training must be given at regular intervals, and details recorded
- The senior manager or director with ultimate responsibility for AML systems and controls, as required by SYSC 6.3.8 is responsible for ensuring that adequate arrangements for training are in place
- The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place.

4.44. There is no single solution when determining how to deliver training; on-line learning can provide an adequate solution but for some staff and volunteers an on-line approach may not be suitable. Procedure manuals can raise staff and volunteer awareness but their main purpose is for reference. More direct forms of training will usually be more appropriate.

4.45. Whatever the approach to training, it is vital to establish comprehensive records to monitor who has been trained, when they received the training, the nature of training given and its effectiveness.

4.46. AML/CTF training and training on the responsibility of staff under the firm's own AML/CTF arrangements must be provided to all relevant employees at appropriate intervals.

Internal controls and record-keeping

4.47. General guidance on internal controls is given in Part I, Chapter 2, and on record-keeping in Part I, Chapter 8. In particular, credit unions must retain:

- copies of any documents or information obtained to satisfy the CDD measures required under the ML Regulations, until five years after the end of the customer relationship
- details of customer transactions for five years after the end of the customer relationship
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report where no external report is made

4.48. Retention of records can be:

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

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

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