Guidance Notes

on compliance with the

Criminal Justice
(Money Laundering and Terrorist Financing)
Act, 2010

Part II

SECTORAL GUIDANCE NOTE

for

CREDIT UNIONS

January 2013

Contents

CREDIT UNIONS

ANTI MONEY LAUNDERING & COMBATING THE FINANCING OF TERRORISM

GUIDANCE NOTE

Introduction

This Guidance Note has been drafted by the ILCU to assist credit unions in their compliance with the provisions of the **Criminal Justice (Money Laundering and Terrorist Financing) Act, 2010** (the "*CJA 2010*") which has as its aim the deterring, detection and disruption of money laundering and terrorist financing activities in a range of financial and other institutions.

It replaces the Guidance Notes issued to credit unions by the Registrar of Credit Unions in July 2004 - *Money Laundering, Guidance Notes for Credit Unions* and guidance issued by the ILCU in 2004 - *Money Laundering, A Guide for Credit Unions*. It is intended that this Guidance will provide credit unions with best practice recommendations around their compliance with the *CJA 2010*. These guidelines do not constitute secondary legislation and credit unions **must always refer directly to the CJA 2010** when ascertaining their statutory obligations. These guidelines are subordinate to the CJA 2010 and to the Core Guidance Notes available from www.finance.gov.ie. The Central Bank has indicated that it will have regard to these guidelines when assessing a credit union's compliance with its obligations under the *CJA 2010*.

Where this Guidance uses the word ***must*** it is referring to a specific legislative or regulatory requirement as outlined by the *CJA 2010*. Where ***should*** is used it is a suggestion as to recommended best practice or regulatory requirements. However, credit unions should bear in mind that their following or failure to follow Guidance may be taken into account by the Central Bank when determining compliance with their money laundering and terrorist financing obligations. Where ***may*** is used in this Guidance the advice is suggested only and may not be a requirement for every credit union.

The *CJA 2010* contains a number of criminal offences applicable to credit unions and their officers. In addition a credit union or its officers may be subject to the administrative sanctions regime of the Central Bank for any failure to comply with the provisions of the *CJA 2010.*

A. WHAT IS MONEY LAUNDERING/TERRORIST FINANCING?

Money Laundering

1 Traditionally money laundering is associated with the process whereby criminals legitimise the proceeds of their crime, for example from drug trafficking, by making it appear to come from a reputable source. This has been achieved via the financial system by opening accounts and undertaking transactions to disguise the origin of the funds. In this way, the normal services of a financial institution such as the credit union are used/abused by the criminal to "wash" the proceeds of their crime. Lately, due to the greater scrutiny of accounts and the transactions passing through banks in particular, criminals have looked at other avenues to launder their criminal proceeds. Criminals are particularly concerned to avoid leaving records of their activity, and their interactions with financial institutions with good anti-money laundering controls are not usually conducive to this.

There are three recognised stages in the money laundering process (placement, layering and integration):

- Placement involves placing the proceeds of criminal conduct in the financial system, i.e. the lodgement of funds into the credit union in large transactions or a number of smaller transactions.
- Layering involves converting the proceeds of criminal conduct into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as loans or investments and very often may have an international dimension, i.e. conversion of currency or transfers abroad.
- Integration involves placing the laundered proceeds back in the economy to create the perception of legitimacy, which may involve purchase of high value goods or property.

Money laundering has more recently seen a growth in large transaction based money laundering, e.g. property purchases/sales, the acquisition of high value goods and their later disposal. In such circumstances the financial institution is less the target of the money launderer but rather may become aware of the transaction due to the services it provides.

2 A number of other factors have also changed the concept of money laundering. Firstly the definition has broadened so that under the *CJA 2010 (S. 7)*; anybody who conceals or disguises the true nature, source, location, disposition, movement or ownership of the proceeds of criminal conduct; or those who convert, transfer, handle, acquire, possess or use that property; or those who remove or bring into the State the proceeds of criminal activity; either knowingly or believing (**or being reckless** as to whether or not) the property is the proceeds of criminal conduct is guilty of an offence. In addition the definition of criminal activity is very wide and includes not only the actual proceeds of the activity itself, but also any additional or intangible benefits (i.e. saved costs) arising from an offence. Finally, the definition of the proceeds of criminal activity has no lower limit, so even quite small amounts arising from criminal activity are regarded as subject to reporting.

3 One significant area that is also covered by this definition is **tax evasion**. The possession of one's own proceeds from the evasion of tax is money laundering. Consequently, where the suspicion arises in the course of the credit union's transactions that the member is evading tax, it must be reported. This would include areas of social welfare fraud or customs offenses in addition to tax evasion. However, in fulfilling its requirements under anti-money laundering legislation, a credit union may reasonably assume that a member has discharged his/her tax liabilities unless there are suspicious activities indicating the contrary. There is no positive obligation on the credit union to establish whether the member has or has not done so.

A 4th EU Directive on anti-money laundering & combating the financing of terrorism (AML/CFT) is anticipated soon to implement the latest 40 recommendations of the Financial Action Task Force (FATF) – the body responsible for setting AML/CFT standards globally. Although not yet enacted into national legislation, credit unions should be aware of the imminent effects of this on their AML/CFT policy & procedures. The major changes which will affect credit unions within the proposed 4th EU Directive are likely to be:

- The extension of PEP status to both domestic PEPs as well as non-domestic, including the extension to more junior political roles that may also be open to corruption, i.e., planning, councillors, etc.

- Reiterating a risk based approach and the need to focus resources where AML/CFT risks are greatest.

- Clear inclusion of tax offences including smuggling and customs and excise offences.

Further details of money laundering definitions are contained within the Core Guidance Notes Section I C.

Combating the Financing of Terrorism

4 The *CJA 2010 (S. 42)* also requires the reporting of suspicions of terrorist financing as distinct from money laundering.

Terrorist activity can be defined as activities which have as their aim the objective to intimidate a population or compel a government to do (or not do) something. This is done by intentionally killing, harming or endangering people, causing property damage or by disrupting services, facilities or systems. Terrorist financing involves those acts that constitute an offence under section 13 of the Criminal Justice (Terrorist Offences) Act, 2005.

5 There are some similarities between the uses made by terrorists and other criminals of the financial system. Like criminal groups, terrorist groups seek to build and maintain financial infrastructures to support their activities. For this purpose, they seek different sources of funding but also seek to obscure the links to the sources of the funds and the terrorist activities supported.

However terrorist financing can differ from traditional money laundering in two key ways:

- The sums needed to fund terrorist attacks are not always large and the associated transactions are not necessarily complex;
- Terrorists can be funded from legitimately obtained income, including charitable donations, and it can therefore be difficult to identify the stage at which legitimate funds become terrorist property.

6 Therefore to combat the financing of terrorism (CFT) a credit union may need to adopt strategies that contrast significantly with its AML strategies, for example, it will need to look more at where proceeds are going rather than where they have come from. Similar to the more established AML regime, a legal obligation to file a suspicious transaction report arises where a credit union officer knows, or forms a reasonable suspicion that a transaction may have the objective of carrying out a terrorist act. Further general guidance on terrorist financing is contained within the Core Guidance Note - Section I D.

7 The offences outlined above in relation to money laundering and terrorist financing are obviously numerous and complicated. However it should be remembered that a designated person under the *CJA 2010*, (i.e. the credit union), is not obliged to prove that an offence as described above has been committed. It need only have a suspicion, or reasonable grounds for a suspicion, in relation to the activity of a member which still exists after reasonable consideration has been made. The credit union is not required to identify which offence it believes the suspicious activity is associated with. Once the matter is reported it is the responsibility of the Gardai and/or Revenue Commissioners to investigate the matter.

Screening of Members for Financial Sanctions Purposes

8 The screening of members for financial sanctions purposes is another important aspect in combating terrorism, although not covered by the *CJA 2010*. EU regulations imposing EU Financial Sanctions in Ireland require, among other things, the freezing of all funds and economic resources belonging to, owned or held by, sanctioned persons or entities and the prohibition of the making of funds or economic resources available to sanctioned persons or entities. The regulations also require that any information which would

facilitate compliance with EU financial sanctions regime be immediately provided to the Central Bank.

9 Fundamentally this requires the checking of new members and the on-going checking of existing members against EU Financial Sanctions lists. An electronic list of financial sanctions currently in force is available for review or download from an official EU website:

http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm

HM Treasury also separately maintains a single up-to-date consolidated list of all UK financial sanctions which is useful as a basis for automated checking at:

http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

10 The Central Bank, by the issuance of EU Financial Sanctions alerts, instructs regulated entities, including credit unions, to carry out a thorough examination of their records and report the findings of such examination to the Central Bank. These alerts are issued quarterly thereby requiring financial sanctions screening to be conducted at least on a quarterly basis. It should be noted however that EU Financial Sanctions obligations are absolute and any, including a single, breach is an offence. Periodic financial sanctions screening is an essential tool especially where it is not feasible for the particular credit union to maintain full-time compliance staff and/or volunteers. On-going monitoring of members and transactions with staff and volunteer awareness of EU Financial Sanctions obligations are therefore essential.

11 The penalties for a breach of financial sanctions legislation are set out in domestic Statutory Instruments and related legislation. Any person guilty of an offence under the relevant Statutory Instrument, including a failure to comply with an Instruction issued by the Central Bank, is liable on conviction to imprisonment and/or a fine. There are significant penalties for failure to comply with financial sanctions obligations including fines in excess of €10 million and/or imprisonment up to 10 years.

Further information on the screening of members for financial sanctions is provided by the Department of Finance and Central Bank via their respective websites. The financial sanctions pages of the Central Bank website are at:

http://www.centralbank.ie/regulation/processes/Intfs/Pages/default1.aspx

B. CHANGES IN LEGISLATION

12 The *CJA 2010* implements the **3rd EU Directive** on the prevention of the use of the financial system for money laundering and terrorist financing and repeals and replaces the **Criminal Justice Act, 1994 (as amended)**. The approach of the 3rd Directive is broadly termed as "risk based" and as such suggests changes in the emphasis of designated bodies anti-money laundering and terrorist financing controls. Many credit unions should find that their well thought out current approach to anti-money laundering and terrorist financing can be easily modified to include compliance with this legislation.

13 Some of the specific newer elements of the *CJA 2010* include:

- More focus on senior management (the board of the credit union) responsibility for anti-money laundering (AML) and combating the financing of terrorism (CFT) controls, including personal liabilities. (*S. 111*)

- More focus on a risk based assessment of the credit unions AML/CFT threats and the management of those threats through adequate policy. *(S. 54(1))*

- More focus on the ongoing monitoring of members as part of "customer due diligence" (CDD) which goes beyond simply identifying members. *(S. 54(4))*

- Identification of the beneficial owner on all accounts *(S. 33(2)(b))* and establishing if a member is acting on their own behalf, including identifying the beneficial owner in all school schemes, clubs and societies.

- Introduction of "enhanced due diligence" (EDD) or specific controls for higher risk circumstances. *(S. 37)*

- Introducing the notion of a "politically exposed person" (PEP) as a higher risk category of member. *(S. 37(1))*

- The requirement to identify members where doubts exist as to "the veracity of previously obtained documentation" – therefore the identification of all active members over time. *(S. 33(d))*

- The requirement to train all board members as well as relevant officers in the credit union. *(S. 54(6-7))*

- Introduction of a stricter and more enforceable standard for the reporting of suspicions. *(S. 42).* This is an objective test of suspicion – i.e. a definition of being "reckless" as to whether or not property represents the outcome of criminal conduct and requiring a report to be made if there are "reasonable grounds" for having a suspicion, i.e. would a reasonable person have been expected to make a report in the circumstances.

- Clear identification and extension of the Central Bank's powers to effectively monitor and take measures, (including administrative sanctions) necessary to ensure compliance with the *CJA 2010 (S. 63)* which is specifically applied to credit unions. *(S. 114(3))*

C. OVERVIEW OF THE CREDIT UNION SECTOR

14 The membership of a credit union is restricted to those individuals who fulfil a specific qualification which is appropriate to the credit union (and as a consequence a "common bond" exists between members) - the **Credit Union Acts, 1997-2012** Section 6. The common bond concept is central to the cooperative ethos of a credit union and is also fundamental to the regulatory regime for credit unions.

15 A credit union offers primarily savings and loan products to its local or associational community, (in addition some credit unions are authorised to offer general insurance products and the possibility of further product development cannot be ruled out). There are limits on the level of savings an individual member can hold in the credit union, which are specified by the Central Bank. The return on savings is linked to financial performance. In addition, there are rules governing a credit union's lending activity which are also specified by the Central Bank.

16 Credit unions therefore presently operate within a restricted, often localised market, providing, at present, simpler financial services to members, not to the public at large. However, this is not to say that credit unions have no risk of money laundering or terrorist financing.

D. MONEY LAUNDERING/TERRORIST FINANCING RISKS IN CREDIT UNIONS

17 On the whole typical credit union financial products and their community ethos do not deliver sufficient functionality or flexibility to be the first choice for large scale money launderers and terrorist financiers.

18 However, the high levels of cash transactions going through credit unions may be one area in particular where there is a higher risk of money laundering or terrorist financing. Specific examples of this can include the making of numerous small payments into an account where the amount of each deposit is unremarkable but the total of all the credits is significant – a process known as 'smurfing', or repayment of larger loans over short repayment periods, or in lump sum payments, where the source of the funds is unclear. In addition as credit unions expand into other products and services they should bear in mind the impact of these new products/services on their AML/CFT policies.

19 The size and complexity of credit unions differ substantially from smaller credit unions that manually process most transactions up to the larger more complex credit unions that rely on far greater levels of automation. The AML/CFT monitoring procedures implemented by individual credit unions will need to reflect this differing level of complexity, with simple manual monitoring systems being used for smaller credit unions and possibly more complex automated systems for larger credit unions.

20 Under the *CJA 2010 (S. 54(2)(a))* credit unions must establish appropriate procedures to identify members and monitor activities, with a particular scrutiny of those that carry a higher risk of money laundering or terrorist financing or those that seem to serve no viable lawful purpose.

Examples of such higher risk activities might include:

- Money transfers to unknown third parties.
- Large one off transactions, particularly in cash.
- Third parties paying in cash on behalf of the member.
- Unusual loan or saving transactions such as larger loans made out to cash or to unexplained third parties.
- Large loans with unexplained short repayment schedules, or the acceleration of the agreed repayment schedule on larger loans (*borrow clean, repay dirty*).
- Reluctance to provide documentary evidence of identity when opening an account (even when taking into account financial exclusion issues).

21 Credit unions also need to be particularly vigilant in the following circumstances:

- The excessive presentation of third party cheques or drafts by members.
- Members taking out larger loans – where funds would seem more readily available and the transaction seems economically unviable.
- Services provided to cash generating businesses, including due care when accepting cash from local businesses, that it represents the true turnover of the business.
- Accounts open with unusual versions of name, or bogus or false names, or requests for multiple accounts for a single member.
- Use of, or requests for, large amounts of high denomination notes (€200 & €500).
- Significant unexplained foreign exchange activity.
- Significant activity in children's accounts where it would seem unreasonable that the child was the beneficiary, (i.e. parents using children's accounts for significant transactions).

- Significant activity in accounts where the only visible income would seem to be welfare support.
- Cash transactions in property deals (domestic or foreign), or significant amounts of cash required to pay suppliers which would be unusual for the service being supplied.

E. APPLYING A RISK-BASED APPROACH IN CREDIT UNIONS

22 In accordance with the guidance presented in Section III of the Core Guidance on the *CJA 2010*, a credit union's risk-based approach will ensure that its strategies are focused on deterring, detecting and disclosing risks of money laundering or terrorist financing in the areas of greatest perceived vulnerability. The credit union may need to take a number of steps, documented in a formal policy statement which assesses the most effectual and proportionate way to manage these money laundering and terrorist financing risks. These steps must include:

- Identifying the money laundering and terrorist financing risks that are relevant to the credit union.
- Assessing the risks presented by the credit union's particular:
    - o Members
    - o Products
    - o Delivery channels
    - o Geographical areas of operation.
- Identification and categorisation of higher risk members. *(S. 37 & S.39)*
- Designing and implementing controls to manage and mitigate these assessed risks. *(S. 54(1))*
- Monitoring transactions, including the large, complex or unusual. *(S. 54(3))*
- Recording appropriately what has been done and why.

See **Annex II** for a sample risk assessment for credit unions.

F. SENIOR MANAGEMENT RESPONSIBILITY AND INTERNAL CONTROLS

23 The credit union board of directors and senior management plays a critical role in the operation of the credit union's AML/CFT system and is ultimately responsible for ensuring an effective internal control structure around AML/CFT. The board should be fully engaged in the decision making process and take ownership of the AML/CFT measures adopted by the credit union.

24 The board in conjunction with management must ensure suitable controls are designed and implemented which must include:

- A formal AML/CFT risk assessment. *(S. 54(2)(a))*
- Customer Due Diligence measures including adequate identification of all members *(S. 33(2)(a))*, and identification of beneficial owners *(S. 33(2)(b))* and Politically Exposed Persons (PEPs). (*S. 37(1))*
- On-going member monitoring procedures *(S. 54(3))* including identification of complex or large transactions and unusual patterns of transactions that have no apparent economic or visible lawful purpose.
- Reporting of all suspicions. *(S. 42)*
- Training of all relevant officers, including all directors. *(S. 54(6-7))*
- Record keeping. *(S. 55)*
- Policies and procedures for the monitoring and management of compliance with the *CJA, 2010*. *(S. 54(4))*
- Internal communication of the policies and procedures above. *(S. 54(4))*

25 Credit unions must have a well-considered AML/CFT policy in place *(S. 54(1))* covering its risk based approach. Such a policy will facilitate a knowledgeable board and well informed staff/volunteers, and will allow ease of effective review by internal or external auditors and regulators. The AML/CFT policy should be reviewed on at least an annual basis. In addition qualified parties who are independent of the implementation of the credit unions AML compliance programme (such as internal audit, external audit or external professionals) may be engaged to review AML/CFT policy and procedures to ensure they are set-up and operating effectively.

26 A credit unions policy will need to take account of its own experience and knowledge of its members and their financial activities. The credit union should also consult the Core Guidance Note and this credit union sectoral Guidance Note when drawing up its policy and systems. As part of its policy, the credit union may wish to include its obligations to check against the various sanctions lists maintained by the Central Bank, EU and United Nations. In addition, the Financial Action Task Force website at www.fatf-gafi.org will keep credit unions up-to-date with money laundering/terrorist financing typologies. Relevant regulator documents relating to money laundering can also be found at www.centralbank.ie and the ILCU www.creditunion.ie provides guidance, policy advice and online training on AML/CFT matters.

27 Following the establishment of a risk-based approach, it is the responsibility of the credit union's Board of Directors 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 should allocate to an officer (likely to be the new *Compliance Officer* - who may or may not also be the money laundering reporting officer, MLRO) overall authority within the credit union for the establishment and maintenance of effective anti-money laundering systems and controls. One of the key tasks of this individual should be the drawing up of an annual report to the Board on the operation of the credit union's

AML/CFT systems and procedures providing a reasoned assessment of the credit union's compliance with AML/CFT legislation and guidance.

28 The *CJA 2010 (S. 111)* ascribes specific responsibility to the board of the credit union for offences committed within the credit union, including liability for the credit unions failings if due to the "*consent, connivance or wilful neglect"* of the board.

G. CUSTOMER DUE DILIGENCE – CDD

29 The *CJA 2010 (S. 31(1))* requires what it terms "Customer Due Diligence" CDD to be applied to all members prior to the establishment of a business relationship with the member and on an ongoing basis thereafter. This requires the following steps:

- Identification and verification of members identity.
- Identification of beneficial owners.
- Obtaining information as to the purpose and intended nature of the account.
- Enhanced Due Diligence where required.
- Conducting ongoing monitoring.

Identification and Verification of Members

30 The anti-money laundering/combating the financing of terrorism (AML/CFT) 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/CFT procedures. Credit unions should be satisfied that the policies and procedures in place for verifying identity are effective and that they make provision for circumstances when increased evidence may be required.

31 For the vast majority of members the standard identification requirement suggested in **Annex I** will be applicable. Credit unions should not however use the *CJA 2010* as a reason to deny service to members who cannot genuinely provide this documentation and attention is drawn to Appendix II of Core Guidance Notes which provides advice on the approach to verifying the identity of customers who are at risk of financial exclusion. Such cases would be dealt with under the **exceptional circumstances** as outlined in **Annex I** of this document.

Documentary Verification

32 Examples of documents that are acceptable for verification of identity are presented in **Annex I**. Credit unions are likely to continue to ask for two standard pieces of documentation before signing up a new member as summarised below:

Identification	**Address verification**
One of the following: • Current Passport • Photo card Driving Licence • National Identity Card • ML 10 Garda Form	One of the following: • Current bill • Current statement • Government issued documentation

33 For **joint accounts** both members should be adequately identified.

34 If there is a **change of name**, i.e., due to marriage or separation, the credit union should establish that the name change is indeed genuine and retain records supporting the reason for the name change, i.e., a marriage certificate or birth certificate. The general principle of one member one account does much to mitigate AML/CFT risks in this respect.

Existing Members

35 The *CJA 2010 (S. 33(1)(d))* requires that CDD be applied to existing customers where there exist:

> *"reasonable grounds to doubt the veracity or adequacy of documents or information previously obtained for the purposes of verifying the identity of the customer."*

This obligation presents significant practical problems for credit unions particularly in obtaining and verifying new identification information in relation to existing members, particularly those who may have joined before the implementation of the original Criminal Justice Act, 1994 and were therefore exempted at the time from obtaining and verifying identity.

36 To meet this new obligation it is recommended that the credit union should review the appropriate identification data held for an existing member in the following **trigger circumstances**:

- The credit union's risk-based assessment of its business indicates that the member in question falls into a higher than standard risk category, such as when moving to a higher risk product or service.
- A member looks for a new product or service, i.e. a new loan application, or moves to a new type of account.
- The member's account has been previously inactive for a certain period of time where this is unusual for the nature of the service being provided.
- A transaction of significance takes place, such as a large lodgment or withdrawal.
- Doubt has arisen in the normal course of business in relation to previously obtained documentation or information.
- Doubt has arisen in the normal course of business that the member, contrary to previous information, is acting on their own behalf.
- The credit union has any suspicion that the member may be involved in money laundering or terrorist financing.

Credit unions may also wish to identify circumstances particular to their own activities which would also trigger the application of CDD to existing members and may also wish to attach a note in AGM materials notifying members of the need to provide up-to-date address details to the credit union.

37 Due to the long-standing relationship between the credit union and existing members the above trigger approach is a reasonable means by which to manage the risk of money laundering. There would not be a rationale for any immediate mandatory overall retrospective establishment and verification of identification for all members.

38 In cases where a member refuses to provide adequate identification as per the guidelines above the credit union should not provide the new service or product to the member. Continued failure by existing members to provide adequate documentation may in itself constitute a reportable suspicion under the *CJA 2010* and could ultimately lead to the need to close the account.

39 The additional requirement under the *CJA 2010* to establish and identify beneficial owners on accounts, (particularly for minor accounts, clubs, societies and companies), applies to accounts irrespective of when they were opened. Therefore if the credit union has cause to doubt the adequacy of identification documentation previously obtained for beneficial owners it may determine that the above triggers, used to identify existing members, should also be used to establish identity for beneficial owners on accounts.

Further details on establishing and identifying beneficial owners are contained under the sections on Clubs, Societies and Company Accounts below.

Industrial Credit Unions

40 Members of industrial credit unions, e.g., civil service, utility, teacher and Garda credit unions, share the common bond of being associated with one particular employer or industry group.

41 Although such employee groups may issue photographic identity cards it is still recommended that such credit unions undertake the same identity verification as outlined in **Annex 1** – principally an independent photographic record and address verification.

42 For industrial credit unions whose common bond extends to family members of employees they should seek the standard verification information from each family member. In these circumstances, credit unions should follow the guidance in **Annex I**.

43 Having the member personally attend the credit union can be difficult for industrial credit unions with a nationwide common bond. In these cases the credit union may wish to rely on certified copies of ID to ensure it is a true likeness of the member joining. It is recommended that a Garda, CPA, Notary, Solicitor, regulated credit institution, JP, Commissioner of Oaths or medical professional be used when certifying identification documents. Credit unions own employer photo ID records may be used to help certify independent photo ID, such as a passport or drivers licence, but should not be used as the primary form of identification. Further details on dealing with non face-to-face identification are presented within the Core Guidance Notes – Section IV.

Credit Union Minor Accounts

44 When opening children's accounts there may be some difficulty in obtaining the standard identification as outlined above. For minor accounts, credit unions should insist on obtaining certification of the child's identity through a passport or **birth certificate** and where the person opening the account is not the Parent/Guardian already identified by the credit union, and then the Parent/Guardian must also be identified in addition to the identity of the child.

45 It is important to monitor minor accounts to ensure that adults are not laundering through the account.

46 Many credit unions have established links with their local schools. For these credit unions, establishing partnerships with local schools is a key part of their long-term community service strategy. Under a risk-based approach in terms of membership profile and low level of activity undertaken by junior savers, credit unions can reasonably assume that children saving small amounts in a savings club set up through a school present a lower risk of the credit union being used for money laundering purposes.

47 In relation to a school savings scheme a credit union may accept a letter or statement from the school, which includes the date of birth and permanent address of the pupil, on the school's letter headed paper to complete standard account opening procedures for the minor. In addition, in cases where a Parent/Guardian has not previously been identified to the relevant standards (because they do not already have an established relationship with the credit union), the identity and address of the Parent/Guardian as the likely beneficiary on the account should also be established and verified.

48 For existing minor accounts where the credit union may not have previously identified the Parent/Guardian/adult on the account it is suggested that the triggers used to identify existing members above may also be used for minor accounts. Where significant balances exist on child accounts consideration should always be given to identifying the Parent/Guardian/adult on the account.

Clubs, Societies and Company Accounts

49 Where credit unions operate accounts for clubs or societies they should first be satisfied as to the name, legal status, place of residence and purpose of the club. They should also verify the identities of at least two elected officials and/or signatories on the account. This would be ascertained through the same procedures as when dealing with ordinary members, (as per Annex I). When any one of the signatories' changes, a new signatory should replace the old signatory and the new signatory should be identified and verified.

50 In addition, the beneficial owner or controller of clubs and societies should be identified and verified as per the standards used for elected officials/signatories. Beneficial ownership *(S. 33(2)(b))* is taken to mean those who own or control in excess of 25% of the shares or voting rights of the club or society, **or otherwise exert control** over the management of the club or society. For example for a GAA club the beneficial owners would be deemed to be the Executive Committee. Where the beneficial owners have not already been identified as elected officers/signatories on the account then they need to be identified and verified as beneficial owners.

51 Care should be taken when dealing with companies as any device that can be used to disguise the true beneficiaries on an account is susceptible to be used for money laundering or terrorist financing.

52 When opening **company accounts** credit unions should ensure that the company is a bona fide company registered in the state (which can be done with a check of the Companies Registration Office). The documents suggested to be used to open a company account are an original or certified copy of the **Certificate of Incorporation** (or Certificate to Trade) and/or the Memorandum and Articles of Association of the company.

53 A list of the company's directors should also be obtained and those authorised to operate the account should be identified as per the account opening procedures for normal members, i.e., their ID and address information recorded, (see Annex I)).

54 For more information on company accounts refer to the Core Guidance Note - Appendix I.

55 Credit unions should also ensure that they understand the **beneficial ownership** structure of the company, i.e., that they establish and verify the identities of all significant shareholders - being those whose shareholding or voting rights is above 25%. (A certified copy of the company's share holding may be used to establish beneficial owners and the standard procedures for normal members **(as per Annex 1**) used to verify identity.). For additional detail on the requirements for identification of a beneficial owner refer to the Core Guidance Notes Section IV and Annex I.

Establishing Purpose and Intended Nature of the Account

56 Credit unions will need to hold sufficient information about the circumstances of members in order to adequately monitor their activity and transactions. As well as identification records this requires ascertaining information from members at the outset as to the purpose and intended nature of the account, *(S. 35)* and as to the source of funds or wealth for the member. This may be best achieved by the establishment and recording of occupation details on credit union application forms.

57 In the majority of cases the nature and purpose of the relationship with the member this may be obvious from the service provided, i.e. mostly savings and smaller personal loans. However in cases where this is not so, say a member's savings dramatically increase because they are operating a pooled Christmas savings club, or a sizeable loan is provided to a sole trader for "business purposes", then additional information should be

obtained by the credit union such as the source of wealth and of funds for the member. *(S. 35(3))*

58 CDD is also about building a relationship with the membership and knowing when to ask the appropriate questions at the appropriate time. Reasonable enquiries of a member as to source of funds, 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 member and does not give rise to tipping-off. Although not a prescriptive list, examples of when additional member information may be needed include a change in circumstances (name, address, or employer), a sudden lump sum payment or a significant 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 such as salary details, and to update member risk profiles which are used as the basis of monitoring member transactions.

59 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 may wish to refer to the risk matrix outlined in **Annex II** when determining the circumstances for standard, increased or Enhanced Due Diligence.

Enhanced Due Diligence

60 There are certain occasions when Enhanced Due Diligence (EDD) will be required. Primarily this is applied to what the *CJA 2010 (S. 37 (1))* refers to as a *Politically Exposed Person* – PEP**.** A **PEP** is classed to be any Non-Republic of Ireland resident who has within the previous year held a prominent public function, i.e. heads of state, high-ranking government or army officials, their immediate families or known close associates. Credit union's common bonds should make it relatively rare to have non-resident PEPs as members. However, particularly in terms of an immediate family member or close associate, it might be quite possible to have a non-resident PEP as a member.

61 Where the credit union has reason to suspect that an individual member may be a non-resident PEP questions may be asked as to the member's personal background, research conducted of publicly known information or a search of the internet used to gain further information. Larger credit unions may wish to consider using the services of private commercial agencies to perform their PEP checking. If doubts exist as to whether a member is a non-resident PEP they should be treated as Enhanced Due Diligence.

62 The *CJA 2010 (S37(6))* outlines specific requirements to be applied in cases where Enhanced Due Diligence is required for PEPs, i.e. approval of membership by the board, determination of source of wealth and increased ongoing monitoring in line with a PEPs higher risk category.

Other Higher Risk Scenarios

63 In such circumstances where the credit union has determined a higher than standard risk of money laundering or terrorist financing it should undertake increased ongoing monitoring of such member accounts, i.e. regular audit and reports.

64 Examples of such higher risk scenarios for members, products, distribution channels or geographic location might include:

- Where a member is involved in high risk businesses, products or services - such as casinos, money service businesses or dealers in high value goods.
- Where a member has been reported to the authorities in the past.
- When there is no face-to-face contact with the member when joining the credit union.
- Where a service is being provided to what a credible source has identified as a high risk jurisdiction (the Financial Action Task Force - FATF maintains a list of such jurisdictions).

65 It is an offence not to follow adequate CDD (Customer Due Diligence) or if applicable EDD in the credit union. Penalty on conviction is a fine or imprisonment for a term not exceeding five years, or both. Breach of CDD requirements may also be a prescribed contravention and form the basis for administrative sanction (up to and including substantial fines) under Part III (C) of the Central Bank Act 1942.

Ongoing Monitoring

66 Credit unions are required to establish a process for monitoring member transactions and activities which will highlight larger, complex or unusual transactions and those which need further investigation *(S. 54(3)(a))*. The basic requirements of a monitoring system for credit unions are that:

- Certain transactions/activities are flagged for further examination.
- These reports are reviewed by the appropriate person within the credit union.
- Appropriate action is then taken based on the findings of this examination.
- A record is kept of these actions.

67 In any system of AML/CFT monitoring, 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 the vast majority of credit unions may be to ensure ongoing monitoring of:

- Deposits or loan repayments (particularly in cash) over a selected threshold.
- The frequency of members' deposits / loan repayments.
- Members whose total transactions within a given period (say a month) exceed a certain monetary threshold.

The amounts and thresholds used by each credit union will vary with the size, location and individual policy of the credit union, from a few thousand Euro up to perhaps several thousand. For larger credit unions that have more complex operational structures a more sophisticated approach to ongoing monitoring utilising their IT system may be considered.

68 The key elements to monitoring are having up-to-date member 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.

69 Also key to a successful monitoring process is ongoing staff and volunteer alertness.

70 Credit unions should be aware that unusual does not always mean suspicious and therefore unusual transactions should not be the routine basis for making reports to the Gardai and Revenue Commissioners. Identifying what is unusual is only the starting point – credit unions need to assess whether what is unusual gives rise to a suspicion of criminal activity and report accordingly.

H. REPORTING

71 All staff and volunteers need to know the credit unions internal reporting process, so that they know how to report suspicious activity. In credit unions, reports will be made directly to the MLRO.

72 Under the *CJA 2010 (S. 42)* all credit union personnel must report when they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or terrorist financing.

73 The making of a report in good faith is not treated as a breach of confidentiality or of any other restriction on disclosure of information imposed by any other legislation. *(S.47)*

74 Credit unions might consider a reporting template in which to standardise and simplify the internal reporting process. Credit unions may also wish to consider the use of secure email of internal reports directly to the MLRO, or the use of their internal IT system, to aid in the timely and confidential reporting of suspicions. A suggested template for a standard internal AML/CFT report is provided in **Annex III.** All credit union personnel must be clear on how and where to make reports.

75 When determining whether to make a report, staff and relevant volunteers may wish to ask themselves the following questions:

- Does the transaction make sense in the context of the member's business or personal activities?
- Is the size of the transaction expected or usual?
- Is the transaction out of proportion to the normal expected income and expenditure of that member?
- Has there been a recent significant change in the pattern of transactions?
- Is the total value of a series of transactions substantial?
- Is the pattern of repayments on a loan consistent with the member's earnings?
- Are there many transfers to high-risk jurisdictions without reasonable explanation?

76 It should be noted that the *CJA 2010* creates an objective test of suspicion which requires reporting where there are "reasonable grounds" for suspecting that another person is engaged in money laundering or terrorist financing. Therefore credit union staff and volunteers may not be able to rely on an assertion of ignorance of the law, or naivety, where this would not be reasonable for a person in their position and with their training. In addition a court or regulator will have the benefit of hindsight in determining whether there existed "reasonable grounds" for a suspicion and therefore a report to have been made.

77 It is therefore advisable that where any doubt exists as to money laundering or terrorist financing that a report is made to the MLRO. If a report has been made and suspicious transactions continue than each suspicion should generate additional reports as per the credit union's internal reporting system.

78 Once a report has been made the reporter's legal obligation under the *CJA 2010* has been met, *(S. 44 (2)).* Internal reports should be treated as extremely sensitive and procedures put in place to respect the confidentiality of the reporter. Such procedures will also have the added benefit of reducing the risk of "tipping off" the member that a report has been made.

Role of the MLRO

79 The role of the MLRO is central to the credit union's AML/CFT reporting process. The credit union must appoint an officer as MLRO whose legal responsibility it is to receive and act upon suspicion reports.

80 It is up to the MLRO to investigate each report and decide whether or not to report internal suspicions to the authorities. However, reports to the authorities must be made as soon as is practicable, i.e. without delay.

81 A formal register should be maintained by the MLRO of all reports received. MLRO's may wish to consider acknowledging those internal reports he/she receives and similarly should insist upon an acknowledgement for all reports they make to the Gardai and Revenue.

82 MLRO Suspicious Transaction Reports (ML1's available from the Garda AML reporting unit) are posted (or in urgent cases can be faxed) to the following two addresses:

An Garda Síochána, Garda Bureau of Fraud Investigation Financial Intelligence Unit Harcourt Square, Harcourt Street Dublin 2 Tel: (01) 666 3714 Fax: (01) 666 3711	Office of the Revenue Commissioners Suspicious Transactions Reports Office Block D, Ashtown Gate, Navan Road, Dublin 15 Tel: (01) 827 7542 Fax: (01) 827 7484

83 If the MLRO decides not to make a report to the authorities, the reasons for not doing so should be clearly documented and retained with the internal suspicion report. All reports should be date stamped when dealt with to establish evidence that they have been inspected.

84 If the MLRO decides to make a report, this must be done promptly and as soon as is practicable. In practice for the vast majority of transactions, this will be after the transaction has occurred. However, if the credit union were suspicious of a transaction in advance, e.g. a member calls to order an unusually large and suspicious quantity of foreign currency, the internal report must be made immediately and the authorisation from the Gardai at the AML unit sought **before** transacting. *(S. 42(7))*

85 The MLRO must also be in a position to act promptly to enquiries from An Garda Síochána, *(S.56(2)).* In practice this may require the home or work contact details of the MLRO being provided to An Garda Síochána and to the Central Bank, as the competent authority charged with oversight of AML/CFT within financial institutions.

86 To aid in the reporting process the identity of the MLRO should be known to staff and volunteers. However, the credit union should ensure their identity is not divulged to the general membership.

87 The Gardai, Revenue and Central Bank should be mindful of the sensitivity of the MLRO's position, particularly in community based credit unions, and should take all necessary steps to protect the position of the reporter.

88 Further details on MLRO reporting are contained within the Core Guidance Notes – Section VII.

89 It is an offence under the *CJA 2010 (S. 42(9))* not to report suspicions of money laundering or terrorist financing within a credit union to the Gardaí and Revenue Commissioners. The penalty for a person who fails to comply with the reporting requirements on conviction is a fine or imprisonment for a term not exceeding five years, or both. However, it is a defence, if an individual has complied with the internal reporting procedures within the credit union i.e. has completed an internal report and submitted it to the MLRO.

AML Compliance Function

90 Credit unions have a number of additional obligations in respect to their AML/CFT compliance set-up and resourcing options. To meet its various obligations under the *CJA 2010 (S.54)* the credit union should establish a specific anti-money laundering compliance function so as to take specific overall responsibility for the effective implementation of the AML/CFT controls required.

91 This function may be performed by the MLRO or more probably by the new *Compliance Officer* created under the Credit Union Acts, 1997-2012, who has overall responsibility for ensuring compliance with all the credit unions various legal and regulatory obligations. It is quite likely that the two functions (MLRO reporting and AML Compliance will ultimately fall under the remit of the same person within the credit union).

92 The person (or persons) to whom overall responsibility for AML/CFT compliance has been allocated should be credible, independent and experienced and should have a level of seniority within the credit union which affords him/her (or them) with both the Board access and the authority necessary to fulfil their roles. As with the MLRO role the AML compliance function role should be specified in writing.

93 Note that in larger credit unions, the Compliance Officer will ultimately occupy a *Controlled Function* (CF) under the Central Bank's *Fitness & Probity*[1] regime and in most other regulated institutions would also hold prime responsibility for AML/CFT compliance.

94 The AML compliance function should report to the Board on a regular basis. The credit union's categorisation of the risk profile of its members and products will determine the frequency for such reports, however, in practice many credit unions have already determined that AML/CFT issues should be a standing item on the monthly board meeting agenda.

95 It is good practice to require the credit union's MLRO/AML compliance function to prepare an annual report for the board, providing a reasoned assessment of the credit union's compliance with its overall AML/CFT responsibilities. Such a report might outline: the number of internal reports received; the number forwarded to the authorities; an analysis of the operation of the credit union's AML/CFT policy and application of its risk based assessment; records of all training taken and generally outline what steps are required to improve or maintain compliance within the credit union.

[1] Phase one of Central Bank's Fitness & Probity regime for credit unions commences July 2013.

Tipping Off

96 Under the *CJA 2010 (S. 49),* credit union personnel must not make any disclosure likely to prejudice an investigation around a report that has been, or is required to be made in relation to a suspicion of money laundering or terrorist financing or that an investigation is being carried out in relation to those suspicions.

97 Refusing to undertake transactions or provide services or the making of requests for further CDD information from the member, should not be considered to be tipping off. Asking as to the source of funds as part of a credit unions AML/CFT policy should also not constitute a tipping off offence. If a credit union is concerned about whether refusal to provide a service or asking as to the source of funds might tip off a member, advice can be sought from the AML unit of the Gardai.

98 A well thought out policy around appropriate communications to members and internal reporting procedures is the credit union's best defence against a possible charge of tipping off.

99 It is an offence to tip off a member that a report has been made or a suspicion exists of money laundering or terrorist financing. Penalty on conviction is a fine or imprisonment for a term not exceeding five years, or both.

I. RECORD-KEEPING

100 Under the *CJA 2010 (S. 55*), credit unions must retain adequate documentation to aid in the successful identification and pursuit of money laundering and terrorist financing and to show compliance with the various elements of the *CJA 2010*. Specifically the credit union must retain the following:

- Copies of, or references to, the evidence they obtained of a member's identity, until five years after the end of the member relationship (copies of ID and address), *(S. 55(2)),* including identities of all beneficial owners *(S. 33 (2)(b))* and identification of any PEPs. *(S. 37)*
- Details of member transactions (often as IT backups) for five years from the date of the transaction. *(S. 55 (3))*
- Records of ongoing monitoring performed by the credit union. *(S. 35(3))*
- An up to date AML/CFT policy including details of the risk assessment performed by the credit union. *(S 54 (2))*

In addition, credit unions should also maintain a record of:

- Any AML/CFT training provided (an annual training register), including details of any assessments.
- Details of reports to the board made on AML/CFT and in particular the Compliance Officer's /MLRO's annual report to the Board.
- Records of decisions on the sending of (or decision not to send) suspicion reports to the authorities.

101 Retention of records requires that relevant documentation be kept by the credit union so as it can be used as evidence in the event of any possible criminal proceedings.

Acceptable methods of retention may include:

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

102 In circumstances where it is not reasonably practicable for a credit union to copy documents used to verify identity in any format described above (e.g. when at a collection point or using agents), a credit union will need to keep a record of the type of document, its number, date and place of issue, so that, if necessary, the document may be re-obtained from its source of issue.

103 The credit union should be aware that records may be required to prove its compliance with its AML/CFT obligations by a range of bodies such as the Central Bank, external auditors, the ILCU and the credit union's own board oversight committee. However to avoid tipping off within the credit union it is advised that the board oversight committee does not have access to the actual MLRO reporting file itself.

104 In relation to internal suspicion reports the following should be recorded:

- All suspicions reported to the MLRO (The MLRO Reporting file).
- Any internal enquiries made in relation to reports.
- All reports forwarded by the MLRO, including details of reports not forwarded to the authorities for five years from the report being made, or from the date of the decision by the MLRO not to report.

105 It is an offence *(S. 55(12))* for a credit union not to keep records in relation to CDD, including identification of members and details of member transactions. Penalty on conviction is a fine or imprisonment for a term not exceeding five years, or both.

106 Credit unions are also reminded that the Central Bank's administrative sanctions may be brought in cases where a credit union has been proven to have failed to keep adequate AML/CFT records.

J. TRAINING

107 Well trained and vigilant officers within the credit union are a vital component in the identification and reporting of money laundering and terrorist financing suspicions. Under the *CJA 2010 (S. 54 (6-7))*, all relevant credit union officers, (which includes all staff and/or volunteers who may have access to potentially suspicious transactions within the credit union), must be instructed on the law and provided with ongoing training on identifying and reporting transactions or activities that may be related to money laundering and terrorist financing.

108 Credit union boards, managers, staff and other relevant officers and volunteers must receive regular and timely information on money laundering and terrorist financing risks within the credit union. This training should ensure that personnel:

- Understand their obligations under AML/CFT legislation, including their personal responsibility to make reports.
- Are made aware of the internal reporting process.
- Understand the CDD measures required of the credit union including the identification and on-going monitoring of members.
- Are trained in the credit union's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions.

The ILCU has produced an **online training programme** that may be used by credit unions to train their personnel in AML/CFT, available at www.culearn.ie and provides classroom and chapter training and seminars on AML/CFT.

109 Training must be given at regular intervals, and details recorded. This should be at least **every year**. Where new staff or relevant volunteers join, AML/CFT training should form part of their induction process.

110 A senior officer with ultimate responsibility for AML/CFT systems and controls (or if the same person, the MLRO or Compliance Officer) should be responsible for ensuring that adequate arrangements for training are in place.

111 The MLRO should also consider the need for specialist instruction in their individual role above and beyond the standard AML/CFT training provided. The ILCU provides training on the role of the MLRO in credit unions, details of which can be found on the ILCU training website, www.culearn.ie.

112 There is no single solution when determining how to deliver training; on-line learning or class room based learning can both provide an adequate solution. Procedure manuals and guidance can help raise staff and volunteer awareness but their main purpose is for reference and they would not constitute formal training as required by the *CJA 2010*.

113 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. This effectiveness can be achieved through such measures as formal assessments.

114 It is an offence not to train credit union personnel in their AML/CFT obligations. A successful defence by a staff member or volunteer of not having been trained could make the credit union itself guilty of the money laundering offence. Penalty on conviction for not training is a fine or imprisonment for a term not exceeding five years, or both.

115 Credit unions are also reminded that the Central Bank's administrative sanctions may be brought into play in cases where a credit union has been shown to have failed to adequately train their personnel in AML/CFT.

116 Further details of the general training requirements for ALM/CFT are contained within the Core Guidance Notes Section IX.

ANNEX I – MEMBER IDENTIFICATION PROCEDURES

Identity
A natural person's identity may be described as a combination of different pieces of information, including:

- Name
- Address (current and past)
- Date of birth
- Place of birth
- Employment and financial history
- Physical appearance

Ordinarily the name (usually verified by a photo ID), residential address and date of birth are sufficient to adequately identify someone.

In terms of the practical verification of identity of credit union members it is considered good practice to obtain an original and copy for record:

- one official government document containing a photo verifying the name (and date of birth), and
- another supporting document from a reliable source verifying their address.

Based upon the credit union's risk assessment of the individual, additional information may be sought for higher risk categories. However credit unions should be mindful that under Data Protection legislation any documentation sought should be relevant and not excessive and not used for any other purpose than for the reason it was taken.

The *CJA 2010* does not require the taking of tax identification numbers from members (however other legislation may require it is taken for another purpose). PPS numbers should not be used by the credit union as a form of identification.

It using individuals to certify documents the following would be considered suitable persons:

- Garda
- Plasticising Chartered & Certified Public Accountant
- Notaries public/practicing solicitors
- Embassy/Consular staff
- Regulated financial institutions
- Justice of the Peace
- Commissioner for Oaths
- Medical professional

If doubts exist over documentation provided the credit union should not take on the member. Under the *CJA 2010* it is down to the credit union to satisfy that they know who their member is.

Identifying Credit Union Members

Verification of Name (& Date of Birth)

One of the following:

- **Passport**
- **Photo Driving Licence**
- **National Identity Card**
- Identification form with photo signed by a member of the Gardai **(ML10)**
- **Birth Certificate** (used for **minors** only & to confirm name changes)

In **exceptional circumstances** and only in cases where the above could not be reasonably expected the following may be considered:

- Instrument of a court appointment (such as liquidator, or grant of probate)
- Identification verification (in writing, signed and on headed paper) from a reputable 3rd party; i.e., employer, school, college, money advisor, solicitor, priest, care-home or shelter manager, probation officer, government office or local authority official
- Garda National Immigration Bureau (GNIB) Card
- Pension travel pass or social welfare card issued by the Department of Social Protection

2. Verification of Address

One of the following:

- Official documentation issued by the **Revenue Commissioners** or **Department of Protection**
- **Local authority document,** e.g. refuse collection bill, water charge bill
- **Account statement,** e.g. bank, credit union, building society, credit card company
- **Utility bill,** e.g. telephone (including mobile), electric, gas, cable
- **Household or motor insurance certificate**
- **Any of the standard ID documents from list 1 above,** i.e. drivers licence (which contains a current address and is not already being used to verify name)

In **exceptional circumstances and only** in cases where the above could not be reasonably expected the following may be considered:

- Address verification (in writing, signed and on headed paper) from a reputable 3rd party; i.e., employer, school, college, money advisor, solicitor, priest, care-home or shelter manager, probation officer, government office or local authority official
- Search of a commercial agency which can confirm address
- Examination of a local telephone directory or available street directory

Notes:

Documents used for verification should be current; i.e. within 6 months. 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.

All documents should be originals where possible. Care should be taken over accepting photocopies or internet downloads. Credit unions 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.

In case of need, consideration should be given to verifying the authenticity of the document with its issuer. Credit unions should also verify the requirement to use forms of identification listed under the exceptional circumstances above, i.e., by establishing that they are being used for a genuine reason such as financial exclusion.

ANNEX II – MONEY LAUNDERING/TERRORIST FINANCING RISK ASSESSMENT

	Standard Lower Risk	Medium Risk	High risk
Member	Well known established members Adequately identified new members	Less well known members. Possible gaps in identification, i.e. out of date address information, Pre 1995 members, Domestic PEPs where known. Cash intensive businesses; i.e. pubs, service stations, gambling firms, dealers in high value goods (car dealers, jewel, art & antique dealers).	Non domestic PEPs Members on Sanctions List (these accounts must be frozen!) *(These accounts likely to be rare in credit unions but must be checked)*
Product or Service	Simple low value savings and loan products General Insurances	Larger transactions, larger share balances and loans More complex products/services; ultimate beneficiary may not always be clear Foreign dimension; use of payment service provider, i.e. western union, or provision of substantial foreign exchange.	More complex very high value type products/services, i.e. wealth management, correspondent banking, complex trust or company structures *(These products not currently offered by credit unions)*
Delivery Channel	Direct to member	Not always face to face; use of telephone and Internet, payments to 3rd parties, i.e. loan cheques made out to 3rd parties, or receipts by one member into multiple 3rd party accounts.	Member not identified face to face Internet only business *(Not currently offered by credit unions)*
Geography	Not close to Border / Port No Foreign Exchange	Foreign exchange or alternate remittance system used extensively. Areas that are known to have high levels of criminality or terrorist activity	Funds to or from high risk jurisdiction; see FATF list of jurisdictions *(Rare in most credit unions)*
Actions required from credit union:	*Standard Identification;* *OK to use exceptional cases ID, i.e. in cases of financial exclusion.* *Minimal ongoing monitoring required.*	*Standard Identification; but take care if relying on exceptional cases ID alone.* *Ongoing regular monitoring required; i.e. reports of transactions/balances lodged over certain thresholds.*	*Enhanced Due Diligence Required;* *Identify source of wealth or funds along with Standard Identification.* *Detailed ongoing monitoring required* *Sign-off from Board may be required before relationship is permitted.*

The above is a sample suggested Red/Amber/Green money laundering/terrorist financing risk analysis for credit unions. It should allow credit unions to identify which circumstances might contain standard, medium or higher risks of money laundering and terrorist financing. Under a risk-based approach, a credit union should focus resources on tackling its identified higher risks (red lights). Also credit unions are reminded that as circumstances change so might their AML/CFT risks. As well as ongoing monitoring, a formal analysis of AML/CFT risks should be undertaken on an annual basis, perhaps as part of the AML Compliance Officer's/MLRO's annual report to the board. This form must be adapted to the credit unions particular circumstances.

ANNEX III - INTERNAL SUSPICION REPORTING FORM

To (Name of Money Laundering Reporting Officer):

Member Details

Member Name:

Member Number:

Address:

Date of Birth:

Date of Account Opening:

Details of Transaction(s)

Amounts:

Destination/Beneficiary:

Date of First Suspicion:

Reason for Suspicion (Please give detailed reasons for your suspicions below):

Report made by

Name:

Date:

Signed:

Ref:

Please ensure that this confidential form is passed promptly to your Money Laundering Reporting Officer.
Do not discuss your report with anyone. Once a report is made in good faith you will have been deemed to have met your money laundering reporting obligations.
This report will remain confidential.