DRAFT GUIDANCE NOTES

On the prevention of the use of property service providers for the purpose of money laundering and terrorist financing
July 2010

These Draft Guidance Notes contain generic guidance that is applicable to all Property Service Providers.

The following DRAFT Guidance Notes were drafted by The Irish Auctioneers and Valuers Institute, The Institute of Professional Auctioneers and Valuers, The Irish Property and Facility Management Association and The Society of Chartered Surveyors together with Deloitte. The DRAFT Guidance Notes have now been submitted to the Minister for Justice, through the PSRA, for approval. Changes may be made as a condition of Ministerial approval. Members will be advised of the position when that approval comes through and of any changes.

Contents

ABBREVIATIONS
SECTION I: EXECUTIVE SUMMARY
Legislation
Guidance Notes
References
Requirements
What's new?
Competent Authority
SECTION II: SCOPE
To whom does the Act apply?
Who is the Customer?
When do the customer due diligence ("CDD") obligations of Act apply?
Exceptions
Existing Customers
Money Laundering
Terrorist Financing
SECTION III: CUSTOMER DUE DILIGENCE
Step 1: Identify and verify the customer's identity
Step 2: Obtaining information on the purpose and nature of the business
Step 3: Conducting ongoing monitoring
Simplified Customer Due Diligence
Enhanced Customer Due Diligence for Non-Resident PEPs
SECTION IV: THE RISK BASED APPROACH
Introduction
Implementing a risk-based approach
Country / Geographic risk
Customer risk
Transaction risk
Financing risk
Variables that impact upon risk
Controls for higher risk situations
SECTION V: RELIANCE ON THIRD PARTIES
Group Introductions
SECTION VI: INTERNAL PROCEDURES
Money Laundering Reporting Officer ("MLRO")
Systems and Controls
SECTION VII: REPORTING SUSPICIOUS TRANSACTIONS
What is suspicious behaviour?
Internal Reporting
External Reporting
Tipping Off
Data Protection
Directions and Orders
Production Orders
SECTION VIII: RECORD KEEPING
SECTION IX: TRAINING
List of Appendices

ABBREVIATIONS

- **AML** – Anti Money Laundering
- **CDD** – Client Due Diligence
- **CFT** – Combating the Financing of Terrorism
- **ECDD** – Enhanced Customer Due Diligence
- **MLRO** – Money Laundering Reporting Officer
- **PEP** – Politically Exposed Person
- **PSP** – Property Service Provider
- **SCDD** – Simplified Customer Due Diligence

Ref

SECTION I: EXECUTIVE SUMMARY

Legislation

1. Recent legislation has introduced changes to the obligations of Property Service Providers (PSPs) in relation to Money Laundering. The new Act is the Criminal Justice Act (Money Laundering and Terrorist Financing) Act 2010, referred to as "the Act" throughout this document. The Act transposes the 3rd EU Anti-Money Laundering Directive.

2. The Act introduces a new **risk-based approach** regime. The objective of a risk-based approach is to focus resources in the areas of higher risk. It also introduces additional customer due diligence requirements, for example, ongoing monitoring and enhanced due diligence requirements for 'politically exposed persons' ("PEPs").

Guidance Notes

3. These Guidance Notes have been drafted by The Irish Auctioneers and Valuers Institute, The Institute of Professional Auctioneers and Valuers, The Irish Property and Facility Management Association and The Society of Chartered Surveyors and are awaiting approval by the Minister for Justice, in accordance with the Act.

4. A court, in determining whether a PSP has complied with the Act, may have regard to the PSP's compliance with these Guidance Notes, and compliance with these Guidance Notes may be used in a court as a defence.

5. These Guidance Notes are recommendations as to good practice, but do not constitute a legal interpretation of the Act. PSPs are recommended to consult their own legal advisers in relation to the interpretation of the Act as needed.

References

6. Articles of the Directive are referred to as "Art" and sections of the Act are referred to as "S" in the left hand column throughout this document.

Requirements

7. The key requirements of the Act are as follows:

   - To identify and carry out ongoing due diligence of clients;
   - To report suspicious transactions;
   - To maintain appropriate procedures and records; and
   - To provide staff with relevant training.

8. A breach of the requirements may result in enforcement. A full list of potential offences and sanctions is included in Appendix 1.

What's new?

9. Customer Due Diligence now includes the requirement to identify the customer on a risk based approach. An understanding of the purpose and nature of any business relationship must be documented and monitored on an ongoing basis. The Act provides exemptions for customers who are financial institutions or public limited bodies and requires enhanced due diligence for customers defined as Politically Exposed Persons.

Competent Authority

10. In the case of PSPs, the relevant competent authority is the Minister for Justice. The Act provides that competent authorities shall effectively monitor and take the necessary measures with a view to ensuring compliance with the obligations imposed.

Designated Person

11. This new Act applies to all designated persons. Designated person means any person, acting in the State in the course of business carried on by the person in the State, who or that is-

S.25(1)

(a) a credit institution,
(b) a financial institution,
(c) an auditor, external accountant or tax advisor,
(d) a relevant independent legal professional,
(e) a trust or company service provider,
(f) a property service provider,
(g) a casino,
(h) gambling activities at a private members' club, or
(i) trade involving cash transactions of at least €15,000.

SECTION II: SCOPE

To whom does the Act apply?

12. The Act applies to Property Services Providers ("PSPs"), which may be defined as a person or company providing property services in or outside the State, including:

S.24 (1)

- The auction of property other than land;
- The purchase or sale, by whatever means, of land;
- The letting of land;
- Dealers in high value goods; and
- Property management services including-
  i. Administrative services and
  ii. The procurement of any combination of the maintenance, servicing, repair, improvement or insurance of a property,

but does not include a service provided by a local authority in the course of the performance of its functions under any statutory provision.

Land includes any estate or interest in land and/or buildings.

Who is the Customer?

13. These Guidance Notes refer to the term "customer", which is deemed to be limited to the party with whom the PSP has entered into a contractual arrangement.

14. The customer can include any of the following:

- A client vendor;
- The purchaser when the PSP is retained to act on the purchaser's behalf;
- The tenant when the PSP is retained to act on the tenant's behalf;
- A real property owner where the PSP is instructed to manage property on behalf of that owner;
- Both the vendor of high value goods where the PSP is retained to act on the vendor's behalf; and the purchaser of high value goods where a buyer's premium is payable to the PSP; and
- The purchaser of high value goods where the PSP is retained by the buyer but does not act for the seller.

When do the customer due diligence ("CDD") obligations of Act apply?

S.33(1)

15. A PSP shall carry out CDD prior to:

- Entering into an ongoing business relationship; or
- Performing any transaction if the total consideration involved is greater than €15,000.

Exceptions

16. Verification of the identity of the customer, and where applicable the beneficial owner, may be completed during, rather than prior to, the establishment of the business relationship if:
    - This is necessary not to interrupt the normal conduct of business; and
    - There is no real risk of money laundering or terrorist financing occurring provided that the verification is completed as soon as practicable after the initial contact.

Art 9 (2)

Existing Customers

17. There may be appropriate documentation on file for existing customers, in which case no further CDD is required.

S.33 (5)

18. The following circumstances in relation to existing customers and existing customer data give rise to a requirement to carry out further CDD:
    - The customer was an existing customer prior to 1994 and as a consequence no CDD information had previously been collected;
    - The customer commences a business relationship; or
    - The customer requests the PSP to provide a new professional service which is considered to present a higher risk of money laundering and/ or terrorist financing.

Money Laundering

Art 1 (2)

19. Money laundering is commonly understood to refer to the processes by which criminals pass the proceeds of their criminal activity through legitimate financial systems to make the money appear to be "clean" or unrelated to crime.

20. The legal definition of money laundering in the Act is much broader than this traditional concept of money laundering as it includes acquiring, possessing or using the proceeds of criminal activity, including the possessing of the proceeds of one's own crime.

S.7(1)

21. As a result, the mere possession, acquisition or use of property, knowing that such property is derived from criminal activity is sufficient for the offence of money laundering to arise even where the objective is not to "cleanse" the asset e.g. handling stolen goods.

22. The scope of the offence is further increased by the very wide definition of property and the fact that the Act contains no de minimus provision. Property may take any form, including in money or money's worth, securities, tangible property and intangible property. As a result, not just proceeds generated by criminal activity are caught by this definition but also:
    - Benefits (e.g. in the form of saved costs) arising from a failure to comply with a regulatory or legal requirement where that failure is an offence e.g. benefits obtained from tax evasion; and
    - Benefits obtained through bribery or corruption, including benefits (such as profit or cash flow) from contracts obtained by these means.

Terrorist Financing

23. Terrorist financing is an offence whereby a person by any means, directly or indirectly, unlawfully and wilfully provides, collects or receives funds intending that they be used, or knowing that they will be used, to carry out an act that constitutes a terrorist offence or for the benefit of a terrorist group.

Art 1 (2)

24. There can be considerable similarities between the movement of terrorist property and the laundering of criminal property. Some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property more generally:
    - Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property; and
    - Terrorists can be funded from legitimately obtained income, including charitable donations, and it can be extremely difficult to identify the stage at which legitimate funds become terrorist property.

S.2 (1)

SECTION III: CUSTOMER DUE DILIGENCE

Art. 8 (1)

25. Customer Due Diligence ("CDD") is intended to enable a PSP to form a reasonable belief that it knows the true identity of each customer. In the normal course of acting for customers, PSPs may also learn surrounding information which may be helpful in terms of AML/CFT, e.g. the source of funding.

S.33

26. It is suggested that in the letter confirming Terms of Engagement, the PSP should note that under the Act, additional proof of the customer's identity may be required at any time during the period of engagement.

27. The PSP's procedures should include the following 3 steps:

1. **Identify and verify the identity of the customer;**
2. **Obtain information on the purpose and nature of the business; and**
3. **Conduct on-going monitoring.**

Step 1: Identify and verify the customer's identity

28. Where the interaction with the customer is on a face to face basis then the PSP should have sight of the original document(s) and appropriate details should be recorded. Where a member of the PSP's staff visits the customer at his home address, the staff member should take details of passport or driving license numbers.

S.33

29. Upon receipt of ID for an individual PSPs should:

- Check any photographs for likeness;
- Check the date of birth compared to the customer's apparent age and other documents;
- Compare the spelling of names and addresses on different IDs;
- Compare the customer's signature with those on the ID;
- Take a copy which should be dated, signed and certified as bearing a good likeness to the customer.

30. In the case of customers who are individuals, the PSP can assume that the individual is acting for himself, unless in the course of the business relationship or in undertaking any activities for the customer it becomes apparent the customer is acting for another person.

31. A PSP may rely on a third party to carry out ID verification as per Section 5 of these Guidance Notes. This may be helpful, in particular, where identification of the beneficial owner in a complex structure is difficult to establish e.g. put an arrangement in place with the relevant solicitor bearing in mind the requirement to ID your customer prior to the transaction.

32. If the PSP is unable to satisfy itself concerning the identity of the beneficial owner on the basis of the verification methods that it considers appropriate given the nature of the customer, then it may not enter into a transaction or commence or maintain a business relationship for that customer and it shall consider whether it should make a report to the Gardai and the Revenue Commissioners.

33. Examples of suitable documentation for identifying individuals, non-face to face requirements, corporates, charities, trusts, partnerships, and clubs and societies are included in Appendix 2. Such documentation should be in a language which is understood by the PSP.

S. 35(1)

Step 2: Obtaining information on the purpose and nature of the business

34. A note should be made as to the purpose of the relationship i.e. a sale, letting or management of a property or land.

S.35 (3)

Step 3: Conducting ongoing monitoring

35. The degree and nature of monitoring by a PSP will depend on the size of the PSP's business, the AML/CFT risks that it has, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny.

36. The degree of monitoring will be based on the perceived risks, the transactions undertaken and the location of the customer and the real property.

Simplified Customer Due Diligence

37. Simplified customer due diligence (SCDD) means that a PSP does not have to identify or verify the identity of the customer, or the beneficial owner, or obtain information on the purpose or intended nature of the business relationship, i.e. exemption from step 1 and 2 above. However, the PSP must continue to monitor such customers (step 3 above).

Art 11

38. SCDD can be applied where the customer is:

S.34(5)

- A credit institution- this includes a bank, building society, post office or credit union;
- A financial institution - this includes other financial services entities, e.g. insurance companies, investment management firms, etc.;
- A company listed on a Regulated Market in the EU; or
- Where the customer is a public body.

Enhanced Customer Due Diligence for Non-Resident PEPs

39. The Act requires enhanced measures to be applied to politically exposed persons ("PEPs") who are resident outside of Ireland, but not PEPs who are resident in Ireland.

Art 13(1)
S.37

40. PEPs are individuals who have, or have had, a high political profile, or hold, or have held, public office including a "specified official" or a member of the administrative, management or supervisory body of a state owned enterprise. As their position makes them vulnerable to corruption, they can pose a higher money laundering risk to PSPs. The definition includes persons holding a prominent position in European Union and international bodies such as the UN, World Bank or IMF. An individual ceases to be regarded as a politically exposed person after he has left office for one year. This definition also extends to members of their "immediate families" and to known "close associates".

41. PEP status itself does not, of course, incriminate individuals or entities, it does, however, put a customer into a higher risk category.

42. PSPs are required to conduct enhanced ongoing monitoring of their business relationship with a PEP.

43. Appendix 3 is a standard form which sets out the information required in relation to the identification of a non-resident PEP.

Close associate

44. A close associate of a PEP includes any individual who has joint beneficial ownership of a legal entity or legal arrangement, or has any other close business relations with the PEP; or any individual who has sole beneficial ownership of a legal entity or legal arrangement set up for the actual benefit of the PEP.

Immediate family member

45. Immediate family member of a PEP includes:
    (a) The spouse or any person who is considered to be equivalent to a spouse of the PEP under the national or other law of the place where the person or PEP resides;
    (b) Any child or spouse of a child of the PEP ;
    (c) Any person considered to be equivalent to a spouse of a child of the PEP under the national law or other law of the place where the person or child resides;
    (d) Any parent of the PEP; or
    (e) Any other family member of the PEP who is of a prescribed class.

Specified Official

46. Specified officials included in the definition of a PEP are as follows:

    (a) A head of state, head of government, government minister or deputy or assistant government minister;
    (b) A member of parliament;
    (c) A member of a supreme court, constitutional court, or other high level judicial body whose decisions, other than in exceptional circumstances, are not subject to further appeal;
    (d) A member of a court of auditors or of the board of a central bank;
    (e) An ambassador, charge d'affairs or high-ranking officer in the armed forces; and
    (f) Officials in an institution of the European Communities or an international body.

SECTION IV: THE RISK BASED APPROACH

Introduction

47. While the majority of transactions carried out by a PSP may be low risk, this section provides guidance as to how a PSP may perform a risk analysis and indeed includes examples of high risk transactions which are detailed below.

FATF RBA Guidance for Real Estate Agents

48. A properly applied risk-based approach should result in a more cost effective use of resources. A risk-based approach ensures that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

49. The greatest risks should receive the highest attention. A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. The most commonly used risk categories are:

    - Country or geographic risk;
    - Customer risk;
    - Transaction risk; and
    - Financing risk.

50. The weight given to each category may vary from one PSP to another. Proportionate procedures should be designed based on assessed risk. An effective risk-based approach involves identifying and categorising money laundering and terrorist financing risks and establishing reasonable controls based on risks identified. A risk analysis should be carried out by a PSP on an annual basis at a minimum. Additional risk analysis may be required should the risk profile of the PSP change e.g. purchase of another business or development of a new service line.

Implementing a risk-based approach

51. While there is no agreed upon set of risk categories for PSPs, the examples provided herein are the most common. There is no one single methodology to apply these risk categories, and the application of these risk categories is intended to provide a strategy for managing potential risks.

FATF RBA Guidance for Real Estate Agents

52. The following risk categories can indicate a higher risk of money laundering or terrorist financing, dependent upon all of the surrounding circumstances, taking into account the norms of the market at any given time.

Country / Geographic risk

53. Potential elements contributing to risk include:

    - Location of property(s) in relation to the buyer. Different countries pose different levels and types of risks pertaining to cross border, non-face to face transactions, e.g. some countries have higher or lower levels of criminality and/or regulation; and
    - Location of the buyer and seller.

54. Factors that may result in a determination that a country poses a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN);
- Countries identified by credible sources as lacking appropriate anti-money laundering/combating the financing of terrorism ("AML/CFT") laws, regulations and other measures. "Credible sources" refers to information that is produced by the Financial Action Task Force ("FATF") and FATF-style regional bodies. Such sources may include, but are not limited to international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units;
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them;
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity; and
- Countries where there is no mandatory registration of real property.

Customer risk

55. The behaviour and motivations of customers may be a source of suspicion, however, PSPs may also form concerns or suspicions about the other parties in a transaction, which may need to be reported to the MLRO, or relevant contact within the PSP.

56. The main customer risk categories are:

- Significant and unexplained geographic distance between the agent and the location of the customer;
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interest;
- Cash intensive businesses;
- Charities and other non-profit organisations that are not registered;
- The use of intermediaries who are not subject to adequate anti-money laundering/combating the financing of terrorism ("AML/CFT") laws and measures and who are not adequately supervised; and
- Politically exposed persons (PEPs).

Transaction risk

57. This category of risk is associated with the factors related to the property, the financing of the transaction and the parties to the transaction:

- Speed of the transaction (transactions that are unduly expedited without a reasonable explanation may be higher risk);
- Successive transactions, especially of same property in short period of time with unexplained changes in value;
- Introduction of unknown parties at a late stage of transactions, e.g. arrangements made between purchasers;
- Third-party vehicles (i.e. trusts) used to obscure true ownership of buyer;
- Under- or over-valued transactions;
- Sale of properties immediately before restraint or insolvency; and
- Property value not in the profile of the customer.

Financing risk

58. Financing risk is associated with the factors related to the funding and/or source of funding relative to a transaction. Potential elements contributing to financing risk include:

- Location of customers and/or customer's source of funds;
- Unusual sources, e.g. funds obtained from unknown individuals or unusual organisations;
- Purchases with large amounts of cash;
- Cash deposits or money orders from unusual sources or countries as identified under country/geographic risks;
- Use of complex loans, or other obscure means of finance, versus loans from regulated financial institutions; and
- Unexplained changes in financing arrangements.

59. PSPs who are involved at any level in the obtaining, processing or closing of a loan, mortgage or other financial instrument must consider the specific risks that raises, and make reference to guidance for financial service providers.

60. PSPs who handle purchase funds must also ensure that their policies and procedures are sufficiently robust to account for the additional risk this poses.

Variables that impact upon risk

61. There are a number of variables that may impact upon these risk categories, dependent upon all of the surrounding circumstances:

- Involvement of other parties, e.g. financial institutions, lawyers or notaries, and whether they are subject to AML/CFT requirements;
- How the customer was introduced to the PSP;
- Method of communication between customer and PSP, e.g. email or personal contact;
- Whether the customer is a PEP;
- Whether there is a beneficial owner that is different from the direct customer;
- The products / services used by the customer; and
- The person with whom the PSP has the relationship, for example legal persons or arrangements with no clear structure might pose a higher risk than a natural person.

Controls for higher risk situations

62. PSPs should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as the result of the agent's risk-based approach. These measures and controls may include:

- Increased awareness by the PSPs of higher risk customers and transactions within business lines across the institution;
- Enhanced due diligence;
- Escalation of the approval process within the PSP;
- Increased monitoring of transactions; and
- Increased levels of ongoing controls and frequency of reviews of relationships.

63. The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that PSPs establish specific controls targeting each and every risk criteria.

Documentation of the risk based approach

64. The risk assessment completed on an annual basis (or more often if required) should be documented and the outcome used to select the appropriate level of customer due diligence to be applied to high, low and medium risk categories of the PSP business.

SECTION V: RELIANCE ON THIRD PARTIES

65. The Act permits the reliance on a "relevant third party" to carry out CDD subject to agreement, however, the requirement to carry out ongoing monitoring cannot be passed onto the third party. A relevant third party may be defined as a person, carrying on business as a designated person -

Art 14

(a) That is a credit institution;
(b) That is a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides foreign exchange, or money transmission, services);

S.40 (4)(a)

(c) Who is an external accountant or auditor and who is also a member of a designated accountancy body;
(d) Who is a tax adviser and who is also a member of a designated accountancy tax or legal body;
(e) Who is a relevant independent legal professional; or

(f) Who is a trust or company service provider, and who is also a member of a designated accountancy body or of the Law Society of Ireland or authorised to carry on business by the Central Bank and Financial Services Authority of Ireland. Note that a PSP is not a "relevant third party" and hence may not be relied upon to outsource CDD.

66. An arrangement with a third party should contain the following information:

- Confirmation that the third party acknowledges that the PSP is relying upon it for CDD purposes other than ongoing monitoring;
- The group of customers for whom the service is outsourced;
- The customer for whom third party reliance is being obtained and
- The nature of CDD that has been carried out.

67. See Appendix 4 for a suggested third party reliance agreement.

Group Introductions

68. Where customers are introduced between different parts of the same group or offices, one member of a group should be able to confirm to another part of the group that the identity of the customer has been appropriately verified. This does not apply to sharing of information from one franchise to another because they are separate legal entities and such an agreement would be a breach of the data protection Act.

SECTION VI: INTERNAL PROCEDURES

Money Laundering Reporting Officer ("MLRO")

69. PSPs are recommended to appoint a Money Laundering Reporting Officer ("MLRO"), who should be a person sufficiently senior to command the necessary authority - ideally a principal or the licensee if a sole trader. If an MLRO is not appointed, an individual should be appointed with the responsibility of reporting suspicious transactions to ensure consistency of approach and completeness of reporting. If an individual is not appointed, all employees/contractors/directors will be individually responsible for reporting suspicious transactions and meeting the requirements of the legislation.

s. 54(4)

70. The MLRO should have responsibility to administer the PSP's money laundering prevention system, to determine whether a customer's identity needs to be secured and retained and to act as a central point of contact with An Garda Siochána and the Revenue Commissioners in reporting suspicions under the Act.

71. A Deputy MLRO may be appointed to act when the MLRO is absent; within reason there must always be a MLRO available to staff.

72. Where a PSP operates in several branches, it may opt for an MLRO in each office or else a central MLRO to act for the entire firm. In the latter event, a senior individual in each branch should have responsibility to report to the MLRO on behalf of the branch.

73. Franchisees are all separate trading entities, and for them to share information on customers with the franchisor's head office, or with each other, for the purpose of money laundering prevention, may breach the Data Protection Act, unless permission is sought from the Data subject (the customer) to pass such information to another entity for the purposes of AML. Sharing of such information amongst franchisees does not qualify for reliance under third party (refer to Section V of these Guidance Notes) hence, the franchisee must get copies of all the documentation. Each franchisee must have its own MLRO.

74. The MLRO should be afforded reasonable access to information that will enable him/her to undertake his/her responsibility.

75. The PSP must keep in a secure place a written record of all matters that have been reported and decisions made.

Systems and Controls

76. The PSP's AML systems and controls should cover:

- Appropriate training on money laundering and terrorist financing to ensure that personnel are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
- Appropriate documentation of the PSP's risk management policies and risk profile in relation to money laundering;
- Appropriate measures to ensure that money laundering risk is taken into account in the day-to-day operation of the PSP, particularly in relation to:
  – the development of new products;
  – the taking-on of new customers; and
  – changes in the business profile;
- Appropriate documented internal reporting procedures to ensure prompt reporting of suspicions of money laundering and terrorist financing; and
- Depending on the complexity of the organisation, it may be appropriate to arrange independent review mechanisms to assess performance of AML/CFT policies and procedures, e.g. internal audit review. At a minimum, there should be appropriate monitoring procedures to assess the adequacy of the systems and controls to ensure that money laundering risks are effectively managed.

SECTION VII: REPORTING SUSPICIOUS TRANSACTIONS

What is suspicious behaviour?

77. PSPs who know, suspect, or have reasonable grounds to suspect that money laundering or terrorist financing is being or has been attempted must report that suspicion to the Gardai and the Revenue Commissioners.

78. The MLRO must review each report and determine whether it gives rise to any of the following in relation to money laundering or terrorist financing activities:

- Knowledge - having knowledge means actually knowing something to be true.
- Suspicion - suspicion is more subjective and falls short of proof based on firm evidence. Case law suggests that suspicion is a state of mind more definite than speculation, but falls short of knowledge based on evidence.
- Reasonable grounds for knowledge or suspicion - this introduces an objective test of suspicion based on what is reasonable to expect of a PSP with their training and position.

79. Examples of situations which may arouse suspicion are included in Appendix 5.

Internal Reporting

80. All PSPs must put in place an internal reporting process.

81. Once a member of personnel has reported his/her suspicion via the internal reporting process, s/he has fully satisfied his/her statutory obligation.

S.44

82. All suspicions reported via the internal reporting process should be recorded.

83. Until such time as the MLRO advises the member of staff that a report has been made to the Gardai or the Revenue Commissioners, further transactions or activity in respect of that customer should be reported in accordance with the PSP's internal reporting process as they arise.

84. A sample internal reporting form is included in Appendix 6.

External Reporting

85. The MLRO must report to the Gardai and Revenue Commissioners any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing. Such reports must be made promptly after the information comes to that person.

Art 22 (1)a

S.42 (1) 86. A sample External Reporting form is included in Appendix 7.

87. Reports in relation to money laundering / terrorist financing suspicions are to be made to :

Garda Bureau of Fraud Investigation
Money Laundering Investigation Unit
Harcourt Square
Harcourt Street
Dublin 2
Tel: +353 1 6663766
Fax: +353 1 666 3798

Office of the Revenue Commissioners
Suspicious Transactions Reports Office
Block D
Ashtowngate
Dublin 15
Tel +435 1890 333 425
http://revenue.ie

Tipping Off

88. PSPs must not disclose to the customer or other third persons that a report has been made to the Gardai in relation to suspicions of money laundering or terrorist financing or that any investigation is being or may be carried out in relation to those suspicions.

S.49

89. An individual who makes a disclosure which is likely to prejudice an investigation, or who falsifies, conceals, destroys, or otherwise disposes of documents relevant to the investigation (or causes or allows this to take place) commits the offence of tipping off.

Data Protection

S.47 90. The disclosure of information in relation to suspicious transactions to the relevant authorities is not treated as a breach of the Data Protection Act 1988 or the Data Protection (Amendment) Act 2003.

Directions and Orders

91. A District Court judge or a member of the Gardai, not below the rank of superintendent, may by notice order a PSP not to carry out a specified service or transaction for a specified period not exceeding 21 days.

S.17-20 92. At any time, a District Court judge may revoke the direction upon the application of a person affected by the direction.

93. A District Court may make an order in relation to the property concerned for the purposes of enabling access to funds for reasonable living and other necessary expenses or for carrying on a business, trade, profession or other occupation to which any of the property relates.

Production Orders

S.63 [Criminal Justice Act, 1994]

94. Where there are reasonable grounds for suspicion, a member of the Gardai can apply to the District Court for materials to be made available.

95. A file must be prepared within the allotted time granted by the District Court and presented to the Gardai accordingly. In certain circumstances, the judge may grant a warrant to authorised officers to enter the PSP's premises in order to obtain access to materials.

S.78

96. It is recommended that anyone required to hand over materials under this section should keep a copy of the materials that are supplied to the authorities.

SECTION VIII: RECORD KEEPING

Art 30

97. Record keeping is an essential component of the evidentiary trail that must be established in order to assist in any investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

s2, Criminal Evidence Act, 1992

98. PSPs must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation.

S.55 (4) S.55 (5)

99. The PSP is required to keep records of the CDD checks carried out for a period of five years from when the business relationship ends. The records must be kept in the State. The PSP should bear in mind their data protection obligations not to keep information for longer than necessary.

100. In addition, PSPs are advised to retain such other records as they deem necessary to show their compliance with the provisions of the Act in relation to internal systems, compliance management and training.

101. The PSP's records should :

- Show the method used to identify the individual/s concerned;
- Retain copies of documents used to do so; and
- Indicate the details of the transaction, including the parties thereto.

102. To satisfy the requirements of An Garda Siochána and the Revenue Commissioners, it is important that records are capable of retrieval without undue delay. It is not strictly necessary to retain documents in their original hard copy form, provided that the firm has reliable procedures for holding records in microfiche, scanned, computerised or electronic form, as appropriate, and that these records can be reproduced without undue delay. A hard copy format will probably prove the most suitable for most PSPs.

103. Where a report of suspicious activity has been submitted to An Garda Siochána and the Revenue Commissioners, or where it is known that a customer or transaction is under investigation, relevant records must not be destroyed without the prior agreement of the authorities even though the statutory time limit of six years may have elapsed.

SECTION IX: TRAINING

Art 35(1)

104. Employees of PSPs must be made aware of the PSP's AML policies and procedures for identification, record-keeping and internal reporting.

105. The effectiveness of the PSP's procedures will depend on the extent to which all staff members appreciate the serious nature of money laundering.

S.54 (6-10)

106. PSPs should train new personnel, as part of their induction programme and provide refresher training annually for all customer-facing staff to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing is taking place.

107. All staff must be given a general appreciation of the background to money laundering. They must also be aware of the legal requirement for the firm to report and of their own personal legal obligations and of the penalties they could face personally should they not fulfil those obligations. They must be made aware of the "tipping off" offence.

108. This training should include details of the PSP's systems for ongoing monitoring of customer business relationships and the role the individual plays in the functioning of that system.

The Appendices to the Draft Guidance Notes listed below are available on the members' area of the IAVI website under "Practice Information-Legislation" as they are too long to include in the magazine.

Appendix 1 - Enforcement Penalties
Appendix 2 - Examples of CDD
Appendix 3 - Sample Non-Resident's Form
Appendix 4 - Third Party Agreement
Appendix 5 - Examples of suspicious behaviour
Appendix 6 - Sample internal reporting form
Appendix 7 - Sample external reporting form