



AN ROINN DLÍ AGUS CIRT AGUS COMHIONANNAIS
DEPARTMENT OF JUSTICE AND EQUALITY

Anti-Money Laundering Compliance Unit

**Criminal Justice
(Money Laundering and Terrorist Financing)
Act 2010 as amended by Criminal Justice
Act, 2013.**

**Overview of the
requirements for
Persons Directing Private
Members' Clubs
*"designated persons"***

**Department of Justice and Equality,
Anti-Money Laundering Compliance Unit,
2nd Floor, 51 Stephen's Green, Dublin 2.
web:** <http://www.antimoneylaundering.gov.ie>
email: antimoneylaundering@justice.ie

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

0

TABLE OF CONTENTS

ABOUT THE CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010	1
INTRODUCTION.....	1
SOME PRINCIPAL ISSUES FOR “PRIVATE MEMBERS’ CLUBS”	2
KEY LEGAL REQUIREMENTS FOR PERSONS DIRECTING PRIVATE MEMBERS’ CLUBS “DESIGNATED PERSONS”	4
A. LEGAL REQUIREMENT TO REGISTER	5
B. REQUIREMENT TO APPLY CUSTOMER DUE DILIGENCE.....	7
C. INTERNAL POLICIES AND PROCEDURES, TRAINING AND RECORD KEEPING	13
D. REQUIREMENT FOR DESIGNATED PERSONS, AND RELATED PERSONS, TO REPORT SUSPICIOUS TRANSACTIONS TO THE GARDA SÍOCHÁNA AND THE REVENUE COMMISSIONERS.....	16
HOW TO MAKE SUSPICIOUS TRANSACTION REPORTS	18
COMPLIANCE MONITORING	19
ABOUT THE DEPARTMENT OF JUSTICE AND EQUALITY ANTI-MONEY LAUNDERING COMPLIANCE UNIT (AMLCU)	19
THE COMPLIANCE MONITORING INSPECTION VISIT	19
WHAT TYPE OF RECORDS MAY BE REQUIRED FOR INSPECTION?	20
THE POWERS THAT MAY BE EXERCISED BY AN AUTHORISED OFFICER	21
CHECKLIST TO ASSIST IN PREPARING FOR INSPECTION	23
FOLLOW UP.....	23

About the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

Introduction

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by the Criminal Justice Act, 2013 ("the Act") commenced on 15 July 2010. The Act transposes the Third Money Laundering Directive (2005/60/EC) and the Implementing Directive (2006/70/EC) into Irish Law, bringing Ireland into line with the most recent revision of the recommendations of the Financial Action Task Force and ensuring that Irish practice is in line with international standards.

The legislation places a number of obligations on certain "designated persons" to guard against their businesses being used for money laundering or terrorist financing purposes. Persons directing private members' clubs where gambling activities are carried on are included as "designated persons" for the purposes of the Act.

The requirements for persons directing private members' clubs where gambling activities are carried on include:

- Registration
- To identify customers and/or beneficial owners
- To report suspicions of money laundering or terrorist financing transactions to An Garda Síochána and the Revenue Commissioners and
- To have specific procedures in place for the prevention of money laundering and terrorist financing
 - These procedures relate to recordkeeping, staff training and the maintenance of appropriate money laundering/terrorist financing procedures and controls.

Registration under the terms of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the Act) relates to the requirements of that Act and has no effect on the legal status of any club as regards gaming statutes.

The overview is intended to alert persons directing private members' clubs to the main provisions of the Act and to understand the legal obligations.

It is important to note that this overview is not a legal interpretation of the Act and must be read in conjunction with the Act and any Guidelines approved under the section 107 of the Act.

Some principal issues for "Private Members' Clubs"

Casinos

Gaming in Ireland is governed by the Gaming and Lotteries Act, 1956. That Act does not make provision for casinos in Ireland and therefore casinos cannot operate legally in the State.

"Private Members' Clubs"

There are a number of "private members' clubs" operating in the State which provide casino type facilities. The clubs are referred to in the Report of the Casino Committee "Regulating Gaming in Ireland" which was published in 2008.

Registration

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 places a requirement on persons directing private members' clubs where gambling activities are carried to register with the Minister for Justice and Equality. Registration under the terms of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the Act) relates to the requirements of that Act and has no effect on the legal status of any club as regards gaming statutes.

Customers of a private members gaming club

The principal premise underpinning this overview is that all persons who engage in gambling activities in a private members' club will be members of that club.

Each club is expected to keep membership details current and available for inspection if requested to do so by an authorised officer of the Department of Justice and Equality Anti-Money Laundering Compliance Unit (AMLCU).

Throughout the Act reference is made to "a customer". In the context of a private members' club, a member who engages in any transaction is automatically a customer for the purposes of the Act.

Transactions

In the context of a private members club at which gambling activities are carried on a "transaction" means:

"the purchase or exchange of tokens or chips, or the placing of a bet, carried out in connection with gambling activities carried out on the premises of the club by a customer of the club"

€2,000 Transaction Threshold

The 3rd EU Money Laundering Directive requires, under Article 10, that all casino customers must be identified and their identity verified if they purchase or exchange gambling chips with a value of €2,000 or more.

Based on the application of the threshold of €2,000 that applies to casinos in the 3rd EU Money Laundering Directive the Department of Justice and Equality is satisfied that a transaction of a value of €2,000 or more in private members club where gambling activities are carried could give reasonable grounds to constitute a risk of money laundering.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

Accordingly, to mitigate against the risk of money laundering for private members' clubs, the Anti- Money Laundering Compliance Unit has applied the EU Directive "Threshold" of €2,000 for transactions in a private members' club setting where gambling activities are carried on.

To copperfasten this approach, The Department of Justice and Equality is preparing an amendment to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 to give full effect to Article 10 and to make provision for the application of this threshold for private members clubs where gambling activities are carried on.

Linked Transactions

The Act requires that customer due diligence measures must be applied when a series of transactions are, or appear to be, linked to each other. In the Private members' club setting these measures should be applied when a transaction or a series of transactions that are or appear to be linked to each other amount to more than **€2,000**.

Designated persons should monitor such transactions with customers (whose identity has been obtained) from the date of the most recent transaction in order to identify customers who may be attempting to split large transactions into several smaller less conspicuous amounts. If a Club recognises that two or more transactions have totalled more than **€2,000** then the CDD obligations should be applied.

It is important to note that the failure of a designated person to comply with the obligations contained in the Act is an offence and a person, if convicted, is liable to a fine or imprisonment or both.

Key Legal Requirements for Persons Directing Private Members' Clubs "designated persons"

It is important to reiterate that this overview is not a legal interpretation of the Act and must be read in conjunction with the Act and any Guidelines approved under the Act. The overview is intended to alert you to the main provisions of the Act for designated persons and to help you understand your main obligations.

It is a matter for every person who directs a private members' club at which gambling activities are carried on to fully familiarise themselves with the requirements of the obligations contained in the Act. The full measures which are to be applied are contained under Chapters 3 to 7 of the Act.

The principal obligations for designated persons can be broadly grouped under the following headings:-

A. Legal Requirement to Register

B. To apply Customer Due Diligence measures

C. To put in place internal policies and procedures, training and record keeping

D. Requirement to report suspicious transactions to the Garda Síochána and the Revenue Commissioners

The headings are briefly explored in the following sections **A**, **B**, **C** and **D** to alert you to your main responsibilities.

You are advised that it is your responsibility to familiarise yourself with the full requirements under the Act.

Further detailed information is available on the Anti-Money Laundering Compliance Unit's (AMLCU) website: - <http://www.antimoneylaundering.gov.ie>

A. Legal Requirement to Register

Persons directing private members' clubs where gambling activities are carried on must register with the Minister for Justice and Equality.

This requirement is provided for in section 109 (1) of the Act:-

109.—(1) A person who is a designated person pursuant to section 25(1)(h) shall register with the Minister in accordance with such procedures as may be prescribed or otherwise imposed by the Minister.

The meaning of "designated person" is provided at section 25 (1) (h) of the Act:

25.—(1) In this Part, "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.....

(h) a person who effectively directs a private members' club at which gambling activities are carried on, but only in respect of those gambling activities

Failure to register is an offence

It is important to note that a person who is required to register and fails to do so will commit an offence under section 109 (2) of the Act and will be liable (a) on summary conviction, to a fine not exceeding €5,000, or imprisonment for a term not exceeding 12 months (or both), or (b) on conviction on indictment, to a fine or imprisonment not exceeding 5 years (or both).

Registration process

The registration process and ongoing monitoring of compliance with the obligations contained in the Act is administered by the Department of Justice and Equality's, Anti-Money Laundering Compliance Unit (AMLCU). The Application for registration form (which should be completed in full) can be downloaded from the forms section of the AMLCU website: <http://www.antimoneylaundering.gov.ie>

Completed forms should be returned to:

**Department of Justice and Equality
Anti-Money Laundering Compliance Unit,
Floor 2, 51 Stephen's Green,
Dublin 2.**

Important sections of the Act dealing with Registration:

- Section 25 of the Act defines the meaning of the term "designated person". The term encompasses any person working in the State who directs a private members' club at which gambling activities are carried on.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

5

- Section 109 of the Act provides, at subsection (1), that a designated person shall register with the Minister in accordance with procedures which the Minister may prescribe.
- Subsection (2) makes failure to register where required an offence and sets out the penalties attached to that offence.
- Subsection (3) details the particulars to be entered into a register to be established and maintained by the Minister for the purposes of this section 109.
- Subsections (4) and (5) prescribe the form the register should take and where the register should be kept.
- Subsection (6) enables the Minister to set down particulars if they relate to the business or regulation of designated persons directing members' clubs.

B. Requirement to apply Customer Due Diligence.

The Act requires the application of "Customer Due Diligence" at specified times and in specific circumstances including measures for:

- Identification and verification of customer's identity
 - Customer Due Diligence (CDD) initially requires the "designated person" to be satisfied as regards the identification and verification of the customer's identity- Know Your Customer.
- CDD also requires the "designated person" to be alert to any activity which could be related to money laundering or terrorist financing and in particular to complex or unusually large transactions and all unusual patterns of transactions and to take guard against such risks. The measures that are to be applied are contained in Chapter 3 of the Act.
- There are special measures to be applied where there is a business relationship which includes the ongoing monitoring of the business relationship see section 35 of the Act.
- Information on the purpose and intended nature of a business relationship with a customer (reasonably warranted by the risk of money laundering or terrorist financing) must be obtained prior to the establishment of the relationship.
- The "designated person" must conduct ongoing monitoring (including scrutiny of transactions and source of funds, etc.) to determine whether they are consistent with their knowledge of the customer and the normal pattern of business.
- As part of the ongoing monitoring process the "designated person" must ensure that all documents, data and information obtained for the purposes of applying customer due diligence are up to date. All such information retained by the designated person should be reviewed at regular intervals to ensure that it is up to date.
- It may also be necessary to reapply or update current information where a transaction is not consistent with the "designated person's" knowledge of the customer and the normal transaction pattern.
- In addition steps must be taken to determine whether a customer or a beneficial owner residing outside the State is a "politically exposed person" or an immediate family member or a close associate of a politically exposed person see section 37 of the Act.
- If a designated person is unable to obtain any required information, as a result of any failure on the part of the customer **no transactions should be conducted**. Further information on the measures to be taken where a customer fails to provide any requested information or documentation is provided at page 12 of this overview. **NB: in such circumstances particular attention must be paid to the obligations to report suspicious transactions to the Garda Síochána and the Revenue Commissioners and the obligation relating to "Tipping Off" see sections 41 to 53 of the Act.**

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

7

Identification and verification of identity of the customer

Customer Due Diligence requires the "designated person" to identify the customer and to obtain documents that will verify the customer's and or beneficial owner's identity.

Identification and verification measures must be applied at the following times:

- a) Prior to establishing a business relationship (S.33 (1) a) which means CDD must be applied whenever a club takes on a new member ***see note below.**
- b) Prior to carrying out a transaction of €2,000 or more.
- c) Prior to carrying out any service if the designated person has reasonable grounds to believe that there is a real risk or suspicion of money laundering or terrorist financing (S.33 (1) (c)).
- d) Where there are doubts about the veracity or adequacy of previously obtained customer identification information (S.33 (1) d).
- e) On an ongoing basis and at appropriate times to existing customers on a risk-sensitive basis.

What measures are to be taken in establishing identity?

Section 33 Subsection (2) of the Act sets out the particular measures which should be applied in establishing customers' identity and beneficial owners connected with the customer or the service concerned. The subsection sets out the kind of documents or information which can be relied upon to confirm the identity of a customer including documents from a government source or a prescribed class or combination of documents.

Documentation from a government source should be provided e.g. passport, driving licence and this should be verified by other documentation such as recent utility bill to confirm address if necessary. Section 33 Subsection (4) sets out the measures which should be applied by a designated person where a customer who is an individual, is not physically present for verification of his or her identity.

*While verification of a customer's identity should, in most circumstances, be undertaken prior to the establishment of a business relationship, such verification may be undertaken during the establishment of the business relationship if there are reasonable grounds to believe that to do so prior to that time would interrupt the normal conduct of business and where there is no real risk that the customer concerned or the service being sought is for the purpose of money laundering or terrorist financing. The approach to be adopted by "designated persons" with regard to identification and verification is illustrated on the following page:

New Members

- 1. New members must produce satisfactory identification documentation.**
- 2. Verification of Identity is required and it should normally be obtained immediately.**

Verification of a customer's identity is required in all cases before a customer or the club carries out a transaction that: -

- o **exceeds the threshold of €2,000** (whether in one transaction or in a series of transactions that appear to be linked) **or**
- o **If transactions raise suspicions in any other circumstance.**

- 3. If verification can not be undertaken immediately the following applies: -**

Whereas verification of a customer's identity should be undertaken when membership is taken out (before a business relationship commences) the Act provides for circumstances where the requirement might interrupt the normal flow of business and the following is provided **but this is permitted only where transaction/s is for an amount less than €2,000 :-**

A. Where there is no real risk, that the customer concerned or the service being sought is for the purpose of money laundering or terrorist financing, the Act permits the verification to be undertaken "during the establishment of the business relationship".

B. In such cases the designated person must verify the identity of the customer or beneficial owner as soon as practicable unless **C** below applies,

C. NB: Identification and verification is required immediately in all cases where a customer or the club carries out a transaction that:

- o **exceeds the threshold of €2,000** (whether in one transaction or in a series of transactions that appear to be linked) **or**
- o **If transactions raise suspicions in any other circumstance.**

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

9

Existing Members

- In all cases any existing members will also be required to produce satisfactory identification documentation which should be verified. This can be obtained during the course of the business relationship as set out above if the threshold is not exceeded.
- Identification and verification is required in all cases where a customer or the club carries out a transaction that:
 - exceeds the threshold of €2,000 (whether in one transaction or in a series of transactions that appear to be linked) or
 - If transactions raise suspicions in any other circumstance.

Measures to be applied in a business relationship and monitoring transactions

In the context of private members' clubs it is reasonable to assume that every customer is a member and has a business relationship with the club on the following basis:-

- that all customers are required to become members of the club where the gambling activities are carried on,
- that by becoming a member of a club it can be reasonably expected that the commercial relationship between the designated person and the customer will be ongoing, and
- the purchase or exchange of chips or tokens can be considered to be commercial relationship between the designated person and the customer.

There are measures to be applied where there is a business relationship between the club and the customer which includes the ongoing monitoring of the business relationship ***see section 35 of the Act***. The steps to be taken by the designated person in relation to this provision are steps that are reasonably warranted by the risk that the customer or the beneficial owner is involved in money laundering or terrorist financing. The steps taken may include determining the source of wealth and of funds involved in the proposed business relationship or in the transaction or transactions and ensuring that approval is obtained from senior management of the designated person.

Information on the purpose and intended nature of a business relationship

Information on the purpose and intended nature of a business relationship with a customer (*reasonably warranted by the risk of money laundering or terrorist financing*) must be obtained prior to the establishment of the relationship. This information may include information relating to the source of the customers funds.

Suspicious activity

Designated persons are required to pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions. It should be apparent if a customer behaves in an unusual manner. Any effort to deviate from what is the normal routine or pattern of customer activity may be enough to alert you to suspicious activity.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

10

Monitoring customer activity and transactions

In its simplest terms, monitoring customer activity and transactions is for the purpose of identifying unusual transactions or customer behaviour that may be linked to money laundering or terrorist financing activity.

Fundamental to a good monitoring system is obtaining and keeping current customer and transaction information. Once this system is established the task of identifying unusual transactions is made easier

A good monitoring system should be capable of:

- Highlighting unusual transactions or customer behaviour for further examination;
- Generating reports in relation to such transactions or behaviour for review;
- Ensuring that appropriate action is taken on the findings of any further examination which may include making a suspicious transaction report.

Designated persons should take a combination of appropriate steps, on the basis of their assessment of the money laundering/terrorist financing risk that each transaction, customer, or class/category of customer, presents, addressing:

- For all customers, determining exactly who the customer is and appropriately verifying that customer's identity; and
- For higher risk customers or transactions, obtaining appropriate additional information to fully understand the customer's circumstances including, where appropriate,
 - the source of the customers funds
 - the expected nature and level of activities
 - keeping records of such information current and valid

As part of the required ongoing monitoring process the "designated person" must ensure that all documents, data and information obtained for the purposes of applying customer due diligence are up to date. All such information retained by the designated person should be reviewed at regular intervals to ensure that it is up to date.

It may also be necessary to reapply or update current information where a transaction is not consistent with the "designated person's" knowledge of the customer and the normal transaction pattern.

- **Please note there are additional requirements for enhanced customer due diligence for Politically Exposed Persons (PEPs)**

Enhanced Customer Due Diligence for Politically Exposed Persons

Please refer to Section 37 of the Act for full details of these requirements.

Section 37 provides that a "designated person" must take steps to determine whether a customer or a beneficial owner residing outside the State is a "politically exposed person" or an immediate family member or a close associate of a politically exposed person.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

11

Subparagraph (9) of Section 37 sets out the meaning of a Politically Exposed Person and a "close associate" and "an immediate family member" of a Politically Exposed Person.

For the purposes of the Act a Politically Exposed Person means an individual who is or was in the preceding year, entrusted with a prominent public function including a member of an administrative, management or supervisory body of a state owned enterprise, a head of state, head of government a government minister or deputy or assistant minister, a member of parliament, a member of a supreme court, constitutional court or other high level judicial body, a member of a court of auditors or the board of a central bank, an ambassador charge d'affairs or high ranking officer in the armed forces.

What happens if the club is unable to obtain the required information or if the customer refuses to provide it?

The obligations for a designated person who is unable to apply the CDD measures are clearly outlined at section 33(8) of the Act;

A designated person who is unable to apply the CDD measures specified as a result of any failure on the part of the customer to provide the documents or information:-

- a) shall not provide the service or carry out the transaction sought by that customer for so long as the failure remains unrectified, and
- b) shall discontinue the business relationship (if any) with the customer.

In addition, where a "designated person" is unable to apply the measures because of a failure of a customer to provide the required information consideration should be given to whether a report to the Gardaí and the Revenue Commissioners should be made. Particular attention must be paid, if a report is made, to the requirements contained in Section 49 which prohibits, a designated person from making any disclosures likely to prejudice any ongoing or future investigation.

It is your responsibility to familiarise yourself with the full requirements of the Act.

C. Internal policies and procedures, training and record keeping

Persons Directing Private Members' Clubs at which gambling activities are carried on are required to manage their risk to ensure that their club is not used as a vehicle for money laundering. They must ensure that policies and procedures are in place to demonstrate the steps the club has taken to safeguard against these risks.

Some examples of the types of policies and procedures to be adopted are provided below. The full provisions relating to these obligations for "designated persons" are contained Chapter 6 of the Act **sections 54 and 55**.

Designated persons are required to have specific procedures in place to provide for the prevention of money laundering and terrorist financing.

The Act requires designated persons to adopt policies and procedures (including training and record keeping) to prevent money laundering and terrorist financing.

Section 54 directs, at subsection (1), that a designated person shall adopt policies and procedures in relation to the designated person's business to prevent and detect money laundering and terrorist financing. Subsections (2), (3), (4), (5) and (6) detail the type of policies and procedures to be implemented.

Each club must develop and adopt policies and procedures to prevent and detect the commission of money laundering and terrorist financing. These policies and procedures should specify the obligations for each club (and all members of staff) particularly the importance of;

- **the assessment and management of risks of money laundering or terrorist financing, and**
- **Internal controls, including internal reporting procedures.**

It is recommended that all such policies and procedures are properly documented and made available as training manuals for staff.

Risk Assessment of money laundering threat to business

Each designated person must assess and identify the risk of their club being used for money laundering or terrorist financing activity. Once this has been done the business must reduce these risks as far as possible. This mitigation will be achieved by putting appropriate procedures and controls in place and monitoring and updating these on a regular basis.

- **NB: IT IS RECOMMENDED THAT YOUR RISK BASED POLICIES AND PROCEDURES ARE DOCUMENTED**

Documenting policies and procedures will assist a designated person to demonstrate to the competent authority that the all the requirements have been met

Policies and Procedures

- **The policies and procedures to be adopted should deal with:-**
 - Risk assessment (as outlined above)
 - Overall management of compliance by the club, internal controls etc.
 - Identification and scrutiny of:-
 - complex or large transactions,
 - unusual patterns of transactions that have no apparent economic or visible lawful purpose,
 - any activity, particularly likely, by its nature, to be related to money laundering or terrorist financing, and
 - measures to be taken to prevent anonymity when dealing with cash transactions (e.g. customer identification and verification).
 - The procedure and process for the reporting of suspicious transactions
 - Record Keeping including procedures applied and information gathered by the designated person in relation to CDD for each customer, cash transactions, monitoring of business relationship.
 - Training for staff.

Training

Staff should be properly instructed on the law relating to money laundering and ongoing training provided to include;

- identifying a transaction or other activity that may be related to money laundering or terrorist financing and
- clear instructions on how to proceed once such a transaction or activity is identified.

Record Keeping

There is a requirement to keep records evidencing the procedures applied, and information obtained in relation to each customer. An original or a copy of all documents used by the designated person for the purposes of verifying the identity of customers or beneficial owner must be kept.

Records evidencing the history of services and transactions carried out in relation to each customer must also be kept.

These records must be kept for a period of not less than 5 years after the date on which the designated person ceases to provide any service to the customer concerned or the date of the last transaction (if any) with the customer, whichever is the later.

Important sections of the Act dealing with internal policies and procedures:

- Section 54, requires designated persons to adopt policies and procedures, training and record keeping to prevent and detect money laundering and terrorist financing.
 - Subsections (2), (3), (4), (5) and (6) detail the type of policies and procedures to be implemented.
 - Subsection (8) sets out the penalties for failure to comply with this section.
- Section 55 requires a designated person to keep records evidencing the procedures applied and information gathered by the designated person in relation to each customer.
 - Subsections (2) to (8) prescribe in further detail the requirements of the section, such as the method of recording and the length of time for which the records must be retained.
 - Subsection (10) provides the penalties applicable for failure to comply.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

15

D.Requirement for designated persons, and related persons, to report suspicious transactions to the Garda Síochána and the Revenue Commissioners

A "designated person", in the course of their business, must report any knowledge or suspicion they have of money laundering or terrorist financing.

- **NB: "TIPPING OFF"** It is important to note that Section 49 of the Act prohibits a designated person from making any disclosures likely to prejudice any ongoing or future investigation.

Reporting of suspicious transactions is covered in Chapter 4, sections 41 to 47 of the Act.

Section 42 (1) of the Act requires a "designated person" and related persons, in the course of their business, to report any knowledge or suspicion they have that another person is engaged in money laundering or terrorist financing.

42. — (1) A designated person who knows, suspects or has reasonable grounds to suspect, on the basis of information obtained in the course of carrying on business as a designated person, that another person has been or is engaged in an offence of money laundering or terrorist financing shall report to the Garda Síochána and the Revenue Commissioners that knowledge or suspicion or those reasonable grounds.

A failure by a customer to provide information may give grounds to report

A failure by a customer to provide information relating to the customer due diligence measures may give reasonable grounds to suspect that another person has been or is engaged in an offence of money laundering or terrorist financing.

42 - (4) For the purposes of subsections (1) and (2), a designated person may have reasonable grounds to suspect that another person has been or is engaged in an offence of money laundering or terrorist financing if the designated person is unable to apply any measures specified in section 33 (2) or (4), 35 (1) or 37 (1), (3), (4) or (6), in relation to a customer, as a result of any failure on the part of the customer to provide the designated person with documents or information

"TIPPING OFF" prohibition on making any disclosure that is likely to prejudice an investigation

It is important to note that Section 49 prohibits a designated person from making any disclosures likely to prejudice any ongoing or future investigation.

- Tipping off is covered in Chapter 5, sections 48 to 53 of the Act.
- All Suspicious Transaction Reports (STR's) should be made to both An Garda Síochána and Revenue Commissioners.

49. — (1) A designated person who knows or suspects, on the basis of information obtained in the course of carrying on business as a designated person, that a report has been, or is required to be, made under Chapter 4 shall not make any disclosure that is likely to prejudice an investigation that may be conducted following the making of the report under that Chapter.

(2) A designated person who knows or suspects, on the basis of information obtained by the person in the course of carrying on business as a designated person, that an investigation is being contemplated or is being carried out into whether an offence of money laundering or terrorist financing has been committed, shall not make any disclosure that is likely to prejudice the investigation.

(3) A person who fails to comply with this section commits an offence and is liable—

(a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(4) In this section, a reference to a designated person includes a reference to any person acting, or purporting to act, on behalf of the designated person, including any agent, employee, partner, director or other officer of, or any person engaged under a contract for services with, the designated person.

How to make Suspicious Transaction Reports

An STR is made by forwarding a completed Standard Reporting Form called an ML 1 Form. It is essential that as much detail as possible is included in the ML 1 Form, including the reasons for suspicion, the value(s) of funds for the particular transactions or series of transactions, etc.

Suspicious Transaction Reports should be forwarded by post to:

An Garda Síochána	Revenue Commissioners
Detective Superintendent, Financial Intelligence Unit (FIU), Garda Bureau of Fraud Investigation, Harcourt Square, Dublin 2	Suspicious Transactions Reports Office Block D, Ashtowngate, Navan Road, Dublin 15

In urgent cases, telephone contact can be made between 9am-5pm and/or, if necessary, an STR can initially be sent by fax and followed up by posting in the original.

An Garda Síochána

Phone No.: 01-6663714

Fax No.: 01-6663711

Revenue Commissioners

Phone No: 01-8277542

Fax No: 01-8277484

Note from an Garda Síochána;

- All STRs made to the Financial Intelligence Unit (FIU) will be acknowledged and feedback will be provided on a six-monthly basis with regard to the status of the Garda investigation.
- If the subject and/or funds cannot be linked with "criminal conduct", the "designated person" will receive feedback to the effect that no further action will be taken by An Garda Síochána.
- If members of An Garda Síochána require the necessary documentation from "designated persons" for evidential purposes, then same will be formally uplifted by way of a Court Order.

NB: Your attention is specifically drawn to the provisions of Section 49 Criminal Justice (Money Laundering & Terrorist Financing) Act, 2010. This relates to the offence of "Tipping Off" whereby it is an offence to make any disclosure "that is likely to prejudice an investigation" to any party other than An Garda Síochána (FIU) and Revenue Commissioners with regard to the making/intended making of an STR.

Compliance Monitoring

About the Department of Justice and Equality Anti-Money Laundering Compliance Unit (AMLCU)

The Anti-Money Laundering Compliance Unit has been established within the Department of Justice and Equality to administer the functions of a competent authority under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

In summary, the principal functions of the Unit are:

1. to administer the authorisation process for Trust and Company Service Providers
2. to administer the registration process for Private Members Gaming Clubs
3. to undertake the general functions of compliance monitoring of those designated persons that are assigned by the Act to the Minister.

The general functions of competent authorities are outlined at s.63 of the Act.

The Compliance Monitoring Inspection Visit

The purpose of the Compliance Monitoring Inspection Visit is:-

- To establish that the designated person (and the club) is complying with its obligations under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.
- To assess the club's AML/TF policies and procedures.
- To prepare a report on the business's compliance for consideration by the competent authority.

Who will carry out the inspection

The inspections are carried by authorised officers, appointed by the Minister for Justice and Equality, and will have in their possession identification and a warrant of appointment.

The authorised officer/s may be accompanied, and assisted in the exercise of the officer's powers (including under a warrant issued under section 78), by such other authorised officers, members of the Garda Síochána or other persons as the authorised officer reasonably considers appropriate.

How is the inspection visit organised?

- Generally, the AMLCU will give advance notice of the date of inspection outlining who should be in attendance for the visit.
- From time to time unannounced inspection visits may be carried out without making a prior appointment. At the time of the inspection the AMLCU will give a reason for the unannounced visit and the authorised officers will formally identify themselves.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

19

The areas covered by the inspection

- Each club will be expected to be in a position to demonstrate to the authorised officer that it is fully compliant with the requirements prescribed by the Act.
- The authorised officer will examine and assess the club's anti-money laundering policies and procedures and the systems that are in place to manage and monitor compliance. It is recommended that policies and procedures are documented.
- The authorised officer may also examine transaction records and related documents to check that the customer due diligence and reporting of suspicious transactions measures are being properly applied and that required records are being maintained.
- Each club will be expected to demonstrate that all relevant staff members are sufficiently trained with regard to the requirements particularly to recognise and deal appropriately with suspicious activity.

What type of records may be required for inspection?

Examples include:

- Anti-money laundering policies and procedures and documents/manuals, and staff anti-money laundering training manuals etc.
- Internal/external audits of compliance with internal anti-money laundering procedures and controls.
- Bank statements relating to relevant business
- Customer/Transaction records
- Evidence of the checks made in line with Customer Due Diligence requirements.
- Generally, documented proof of the steps taken and copies of references and other material checked to confirm and verify customers' identity.
- Supporting records for the ongoing monitoring of customer due diligence measures.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

The powers that may be exercised by an authorised officer

- Section 75 confers on authorised officers the power to enter premises and sets out the circumstances in which this power may be exercised.
- Section 77 (1) sets out the activities which an authorised officer may undertake on lawfully entering a premises.
- Section 77 (2) requires a person to whom a request is made in to comply with the request where possible and give such assistance and information to the authorised officer as is reasonable.

77. — (1) An authorised officer may, at any premises lawfully entered by the officer, do any of the following:

- a) inspect the premises;***
- b) request any person on the premises who apparently has control of, or access to, records or other documents that relate to the business of a designated person (being a designated person whose competent authority is the State competent authority who appointed the authorised officer)—***
 - I. to produce the documents for inspection, and***
 - II. if any of those documents are in an electronic, mechanical or other form, to reproduce the document in a written form;***
- c) inspect documents produced or reproduced in accordance with such a request or found in the course of inspecting the premises;***
- d) take copies of those documents or of any part of them (including, in the case of a document in an electronic, mechanical or other form, a copy of the document in a written form);***
- e) request any person at the premises who appears to the authorised person to have information relating to the documents, or to the business of the designated person, to answer questions with respect to the documents or that business;***
- f) remove and retain the documents (including in the case of a document in an electronic, mechanical or other form, a copy of the information in a written form) for the period reasonably required for further examination;***
- g) request a person who has charge of, operates or is concerned in the operation of data equipment, including any person who***

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.

21

has operated that equipment, to give the officer all reasonable assistance in relation to the operation of the equipment or access to the data stored within it;

h) secure, for later inspection, the premises or part of the premises at which the authorised officer reasonably believes records or other documents relating to the business of the designated person are located.

Checklist to assist in preparing for inspection		
	Will you be in a position to give brief overview on anti-money laundering policies/procedures in your club and comment on how the policies are working?	Y N
	Some examples of the policies and procedures that may be examined and assessed:-	
	➤ Assessment and management of risks of money laundering to the club	
	➤ Identification of customers and beneficial owners.	
	➤ Special measures applying to business relationships	
	➤ Enhanced customer due diligence — politically exposed persons.	
	➤ Discretion to apply additional enhanced CDD.	
	➤ Reliance on other persons to carry out customer due diligence.	
	➤ Internal controls & procedures relating to reporting of suspicious transactions to An Garda Síochána/Revenue.	
	➤ Measures to prevent "Tipping Off."	
	➤ The identification and scrutiny of complex or large transactions	
	➤ Keeping of records	
	➤ Training to ensure that persons involved in the conduct of the club are <ul style="list-style-type: none"> a) instructed on the law relating to money laundering and terrorist financing, and b) Provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified. 	

Follow up.

- Once the inspection has been completed, where possible, any immediate areas of concern will be conveyed to you orally.
- As soon as possible following the inspection we will inform you, in writing, of any action that you need to take to ensure that you are in full compliance with the law.
- Unless there has been a serious breach that requires immediate action by you we will endeavour to give you reasonable time to provide any information or to make the necessary improvements.
- It may be necessary to schedule a return inspection which will concentrate on the areas of concern identified.
- It should be noted that failure to comply with the requirements contained in the Act could result in prosecution.

Note: This overview should be read in conjunction with the Acts and any Guidelines approved under the Acts.