



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

AMLCU INFOSHEET 3

## High Value Goods Dealers (HVGDD)

Overview of the requirements for businesses that accept cash payments (of €15,000 or more) for goods in the normal course of business

<b>INTRODUCTION</b>	2
<b>THE LEGAL REQUIREMENTS FOR HVGD "DESIGNATED PERSONS"</b>	3
<b>THE MAIN OBLIGATIONS</b>	4
<b>A. CUSTOMER DUE DILIGENCE (CDD)</b>	5
<b>B. SUSPICIOUS TRANSACTION REPORTS</b>	7
<b>C. INTERNAL POLICIES AND PROCEDURES, TRAINING AND RECORD KEEPING</b>	8
<b>COMPLIANCE MONITORING OF HVGDS</b>	11
<b>ABOUT THE DEPARTMENT OF JUSTICE AND EQUALITY ANTI-MONEY LAUNDERING COMPLIANCE UNIT (AMLCU)</b>	11
<b>THE COMPLIANCE MONITORING INSPECTION VISIT FOR HIGH VALUE GOODS DEALERS</b>	11
THE POWERS THAT MAY BE EXERCISED BY AN AUTHORISED OFFICER	14
CHECKLIST TO ASSIST IN PREPARING FOR INSPECTION	16
FOLLOW UP.	16

## Introduction

This brief overview of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 is intended to alert persons trading in goods, who accept cash payments of €15,000 or more for goods, to the main provisions of the Act and its obligations.

The Act is available from the Government Publications Sales Office and a copy and further information can be viewed at: - <http://www.antimoneylaundering.gov.ie>.

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010<sup>1</sup> introduced important changes to the law for <sup>2</sup>"designated persons" including businesses that accept cash payments for goods in the normal course of business. This sector is diverse and includes such businesses as antique dealers, boat or car sales businesses and dealers in precious stones and jewellers. For ease of reference the sector is referred to as **the High Value Goods Dealer (HVGD) sector**.

*Section 25.—(1) (i) any person trading in goods, but only in respect of transactions involving payments, to the person in cash, of a total of at least €15,000 (whether in one transaction or in a series of transactions that are or appear to be linked to each other).*

The Act places a number of obligations on "designated persons" (businesses), including High Value Goods Dealers, to guard against their businesses being used for money laundering or terrorist financing purposes.

**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.**

The Anti-Money Laundering Compliance Unit (AMLCU) 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. The Unit's compliance monitoring functions will involve making contact with designated persons to ensure that they are meeting their requirements under the Act. Authorised officers have been appointed by the Minister to carry out inspections of premises at which the business of a designated person is carried on.

The measures which are to be applied are contained under Chapters 3 to 7 of the Act and are briefly explored in this overview. Further information is available from the Department of Justice and Equality, Anti-Money Laundering Compliance Unit, 2nd Floor, Bishops Square, Redmond's Hill, Dublin 2.

<sup>1</sup> (referred to as "the Act" throughout this overview)

<sup>2</sup> Section 25.—(1) (i) of the Act

# The Legal Requirements for HVGD "designated persons"

The Act places a number of obligations on "designated persons" (businesses), including High Value Goods Dealers, to guard against their businesses being used for money laundering or terrorist financing purposes. It is important to note that there are specific requirements for "designated persons" depending on the type of customer and the nature of the cash sale.

**The most important obligations placed on a "designated person" who accepts cash payments for goods apply when the total amount of money paid by the customer in the single transaction or series is greater than €15,000. In these circumstances the "designated person" must apply the customer due diligence (CDD) measures specified in *section 33 (2)* and, where applicable, *section 33 (4)* of the Act.**

- The CDD measures include identifying and verifying the identity of all customers and monitoring ongoing transactions where there is a business relationship. **Section 33 (1)** prescribes the times and circumstances when CDD must be applied.

**Generally customers of a High Value Goods Dealers will fall into the following categories:-**

**A. Business Relationship-** "*business relationship*", where there is an expectation of an ongoing commercial relationship (e.g. trade between car dealers for cash or fleet sales).

OR

**B. Occasional Customer -** "*occasional transaction*", with no expectation of ongoing commercial relationship.

## **Section 24 (1)**

*"business relationship", in relation to a designated person and a customer of the person, means a business, professional or commercial relationship between the person and the customer that the person expects to be ongoing.*

*"occasional transaction", in relation to a customer of a designated person, means a single transaction, or a series of transactions that are or appear to be linked to each other, where—*  
*(a) the designated person does not have a business relationship with the customer, and*  
*(b) the total amount of money paid by the customer.*

## **The Main Obligations for HVGDs**

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

### **A. Customer Due Diligence (CDD)**

- Identify and verify customer's identity
- Be alert to suspicious activity
- Monitor ongoing business relationship

### **B. Suspicious Transaction Reporting**

- Report suspicious transactions (STR) to the Garda Síochana and Revenue Commissioners
- NB: "Tipping Off" STR can not be disclosed

### **C. Internal policies and procedures, training and record keeping**

- Including:- Risk assessment, Management of Compliance, Procedure for STRs, Record Keeping, and Training.

The headings are briefly explored in the following sections A, B and C 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. Customer Due Diligence (CDD)

**Customer identification and verification is required when the total amount of money paid by the customer in a single transaction (or series) is greater than €15,000.**

The first legal obligation on “designated persons” is to apply Customer Due Diligence (CDD) procedures as prescribed in **section 33** of the Act to their customers in specific circumstances and at certain times. The full provisions relating to the customer due diligence obligations for “designated persons” are contained Chapter 3 of the Act **sections 33 to 40**.

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 **section 33(2)** 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.

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 9 of this overview. 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**.

### **Know You Customer**

Knowing your customer and conducting business in the normal fashion are probably the key means of preventing money laundering. In respect of your customer, assess the risk and satisfy yourself of the identity and source of funds. **A good risk assessment policy and procedure is vital.**

### **Customer identification**

Customer Due Diligence requires the “designated person” to identify the cash customer and to obtain documents that will verify the customer’s and or beneficial owner’s identity.

Documentation from a government source should be provided e.g. passport, driving licence and this should be verified by a recent utility bill to confirm address if necessary **Section 33 (2) (a)** and **33 (2) (b)**. If the purchaser or beneficial owner is a company or other legal entity steps must be taken to confirm that the entity is bona fide. Records must be maintained of the steps taken to verify identity and copies of documents retained. This process must also be followed for any beneficial owner of the goods.

### **Unusual customer behaviour**

It should be apparent to you when a customer behaves in an unusual manner. Business transactions are normally quite routine and any effort to deviate from routine may be enough to alert you to suspicious activity. In retail cash transactions there should be a clear source of funds e.g. Bank or Credit Union Loan, withdrawal from account etc.

### **Obligation to Keep Records on Identification procedures and transactions**

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.

## B. Suspicious Transaction Reports

There is a statutory obligation on “designated persons” to make suspicious transaction reports to the Garda Síochána and the Revenue Commissioners if he/she suspects that another person has been or is engaged in an offence of money laundering or terrorist financing. Further details are contained at page 10 of this overview.

The full provisions relating to these obligations is contained in Chapter 4 of the Act “*Reporting of suspicious transactions and of transactions involving certain places sections 41 to 47*” .

### **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.

*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.*

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

## C. Internal policies and procedures, training and record keeping

There are obligations on “designated persons” to adopt policies and procedures to prevent and detect the commission of money laundering and terrorist financing. These policies and procedures include internal controls; risk assessment, internal reporting procedures for suspicious transactions and monitoring the management of the controls and some details 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.***

### ➤ Risk Assessment of money laundering threat to business

Each designated person must assess and identify the risk of their business 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.

### ➤ The policies and procedures to be adopted should deal with:-

- Risk assessment (as outlined above)
- Overall management of compliance by the business
- 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.

**IT IS RECOMMENDED THAT ALL POLICIES AND PROCEDURES ARE DOCUMENTED**

## What happens if a designated person 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;

**Section 33 (8):** *A designated person who is unable to apply the measures specified in subsection (2) or (4) 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 required under this section—*

*(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.*

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.

**Section 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.*

**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.*

Particular attention must be paid, if a report is made, to the requirements contained in Section 49 which prohibits, at subsections (1) and (2), a designated person from making any disclosures likely to prejudice any ongoing or future investigation.

## 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:**

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

**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 of HVGDs

### 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 the Minister as 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 for High Value Goods Dealers

#### ***The purpose of the Compliance Monitoring Inspection Visit is:-***

- To establish that the business is complying with its obligations under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.
- To assess the business'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, advance notice will be given to the business to be inspected by the AMLCU 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.

***The areas covered by the inspection***

- Each designated person 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 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 business 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.

**CASH TRANSACTION RECORD**

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

**Part 1 Name and details of person making the cash payment for goods**

Surname

First name

Company name if appropriate

Date of transaction

**Address**

**Part 2 Details of the Cash Payment or series of linked payments**

Amount €  Currency & note denominations

**Part 3 Beneficial Owner details ( if person making payment is not the beneficial owner)**

Surname

First name

Company name if appropriate

**(verification of identity is also required for beneficial owner)**

Address

**Part 4 Customer Due Diligence**

**\*Copies of documents used to verify identity must be kept by the HVG D**

Type of identity document/s

Document Number  Issued by

Expiry date of document:

**Documentation verified:**

**Part 5 Description of goods purchased (please include total value of goods)**

Transaction conducted by name

Verified by Manager - name

Signed on behalf of Company

**SUGGESTED CASH TRANSACTION RECORD -**

## **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 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 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.

**(2) A person to whom a request is made in accordance with subsection (1) shall—**

(a) comply with the request so far as it is possible to do so, and

(b) give such other assistance and information to the authorised officer with respect to the business of the designated person concerned as is reasonable in the circumstances.

**(3) A reference in this section to data equipment includes a reference to any associated apparatus.**

(4) A reference in this section to a person who operates or has operated data equipment includes a reference to a person on whose behalf data equipment is operated or has been operated.

<b>Checklist to assist in preparing for inspection</b>		
<b>You should be in a position to give brief overview on anti-money laundering policies/procedures in your business and comment on how the policies are working?</b>		
<b>Some examples of the policies and procedures that may be examined and assessed:-</b>		
➤ Assessment and management of risks of money laundering to the business		
➤ Identification of customers and beneficial owners.		
➤ Special measures applying to business relationships (and verification of).		
➤ 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 business are <ul style="list-style-type: none"> <li>a) instructed on the law relating to money laundering and terrorist financing, and</li> <li>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.</li> </ul>		

**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.



**Department of Justice and Equality,  
Anti-Money Laundering Compliance Unit,**  
2nd Floor, Bishops Square, Redmond's Hill, Dublin 2.  
Web: <http://www.antimoneylaundering.gov.ie>  
Email: [antimoneylaundering@justice.ie](mailto:antimoneylaundering@justice.ie)