# Brokers Ireland Guidance on the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

# and

# Criminal Justice (Money Laundering and Terrorist Financing (Amendment) Act 2018

**JAN 2019**

## What is Money Laundering?

It is the process by which criminals conceal the true origin and ownership of the proceeds of drug trafficking or other criminal activity.

## Stages of Money Laundering

There are three stages in the money laundering process:

1. Placement – this is the physical disposal of cash,
2. Layering – the creation of complex layers which make tracking transactions difficult,
3. Integration – absorbing the money back into the economy as legitimate money.

## The Offences

- Money laundering – the actual process of laundering money;
- Assisting a money launderer – assisting somebody who is trying to launder money;
- Failure to identify a client – take reasonable steps to identify the client;
- Failure to keep records – records must be retained for five years after the client's last transaction, or the relationship with the client has ended;
- Failure to report – reports must be made to the firm's Money Laundering Reporting Officer, who in return makes a report to the Financial Intelligence Unit (FIU) and the Revenue Commissioners, if appropriate;
- Tipping off – this refers to tipping-off a potential money launderer that his/her activity has been spotted;
- Failure to conduct, document, review and manage a business risk assessment;
- Failure to apply enhanced customer due diligence measures when dealing with customer established or residing in a high-risk third country;
- Failure to apply enhanced customer due diligence measures when there is reasonable grounds to believe that a customer is a Politically Exposed Person;
- Failure to apply enhanced customer due diligence measures where a business relationship or transaction presents a higher degree of risk;
- Failure to investigate complex or unusually large transactions or unusual patterns of transactions in greater detail and increase monitoring if they appear suspicious;
- Failure to adopt and document, review and manage internal policies, controls and procedures and to train relevant staff.

## Maximum Penalties

Individuals and Corporate bodies can have sanctions imposed if they fail to comply with the law. This extends to insurance, investment, mortgage brokers and their employees. The maximum penalties are an 'Unlimited Fine' plus:

- Fourteen years in jail for money laundering or assisting a money launderer.
- Five years in jail for failure to identify, failure to keep records, failure to report or tipping-off.

## What is Terrorist Financing?

A person commits the offence of 'terror financing' if they by any means, directly or indirectly provide, collect or receive funds intending that they be used or knowing that they will be used, in whole or in part in order to carry out:

- An act of terrorism as defined by law, or
- An act intended to cause death or serious bodily injury to a civilian and the purpose of which is, to intimidate a population or to compel a government or an international organisation to do or abstain from doing any act.

It can also include colleting or receiving funds intending that they be used or knowing that they will be used for the benefit of a terrorist group. An Garda Síochána can freeze and/or confiscate funds

used or allocated for use in connection with an offence of financing terrorism or funds that are the proceeds of such an offence.

There can be similarities between the movement of terrorist property and the laundering of criminal property. 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, and
- Terrorists can be funded from legitimately obtained income and it is therefore difficult to identify the stage at which legitimate funds become terrorist property used for terrorist financing.

### Why do Intermediaries have responsibilities?

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended 2018, applies to mortgage, investment and life Intermediaries. Intermediaries who fall under the scope of the Legislation are deemed to be "Designated persons".

Non-life intermediaries are outside the scope of the requirements. However, they are expected to be mindful of other legislation that would apply such as Financial Sanctions, and to have controls and procedures in place to detect and prevent financial crime, and as a result, to report suspicious transactions. Staff would need to be trained also in this regard. See Appendix 6 for further guidance.

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended 2018, introduced the concept of a risk based approach to managing and mitigating money laundering and terrorist financing risks faced by the designated person. Designated persons are required to have the necessary procedures and record keeping processes in place to comply with the legislation.
Intermediaries are required to carry out Customer Due Diligence:

- prior to establishing a business relationship with the customer.
- prior to carrying out for/with the customer any transaction which appears linked to another transaction or prior to assisting the customer in carrying out a single transaction if:
  (i) Currently there is no business relationship with the customer; and
  (ii) The total amount of money paid by the customer in the single transaction or series of transactions is greater than €10,000.
- prior to carrying out any service for the customer, if there are reasonable grounds to believe that there is a real risk that the customer is involved in money laundering or terrorist financing.
- if there are grounds to doubt the veracity of documents provided by the client.
- at any time, including situations where the relevant circumstances of a customer have changed, where the risk of money laundering/terrorist financing warrants its application.

### What does identification mean?

### Personal customers:

Identification of a personal customer is the process whereby a designated person obtains from a customer the information necessary for it to identify who the customer is. The identity of an individual has a number of aspects at any point in time, all of which must **be obtained by the designated person:**

a) name (which may change due to particular events);
b) address (which is likely to change from time to time); and
c) date of birth (which is a constant).

Where a person purports to act on behalf of a customer, a designated person will be obliged to verify

a) the identity of that person, and
b) that they are authorised to so act.

## Legal persons and arrangements:

| Identify | Who to identify: | How to identify: | How to verify: |
|---|---|---|---|
| Customer - legal person or arrangement | Legal person or arrangement | Obtain information from the customer or from reliable, independent source on:<br>i) name, legal form and proof of existence;<br>ii) the powers that bind and regulate the legal person or arrangement;<br>iii) the address of the registered office (where applicable) and main place of business; and<br>iv) the nature of the business and its ownership | This could generally be satisfied by either<br>✓ A search of the relevant company or other registry (where the necessary information is publicly accessible and considered by the Designated Person to be current and reliable); or<br>✓ A copy, as appropriate to the nature of the entity, of the certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other official documentation proving the name, form and current existence of the customer.<br>✓ In cases regarded by the Designated Person as higher risk, use of more than one source of information may be warranted. |
| Customer - legal person or arrangement | Directors (or the equivalent in for example; Partnerships and unincorporated businesses, Clubs, Societies, Public Sector bodies.) | Identify the directors of the legal person or trustees of a trust (or other equivalent persons for other forms of legal entity or arrangement). This information can be provided by the customer or obtained from a reliable, independent source. | This could generally be satisfied by either<br>✓ obtaining a copy of the annual audited accounts listing directors (where the necessary information is publicly accessible and considered by the Designated Person to be current and reliable); or<br>✓ relevant and up-to-date legal opinion from a reliable source documenting due diligence conducted, including in relation to |

| | | | |
|---|---|---|---|
| | | | information on directors; or<br>✓ obtaining information from relevant company or another registry such as the CRO or known foreign equivalent; or<br>✓ as warranted by the risk, verify one or more directors in line with requirements for personal customers |
| Customer - legal person or arrangement | Authorised signatory | Identify the signatories by reference to the duly-approved mandate provided by the customer in relation to the operation of the business relationship. | In accordance with normal business practice and as warranted by the risk of money laundering or terrorist financing, verify the personal identity of one or more of the signatories in line with the requirements for personal customers. Verification of authorised signatories may not be required where a sufficient number of directors have been verified in accordance with requirements |

## Business Risk Assessment

The 2018 Act introduces a requirement for designated persons to conduct a 'business risk assessment' to identify and assess the risks. Intermediaries therefore must assess the level of risk of money laundering/terrorist financing involved in carrying out their own business activities.

Various specified risk factors must be taken into account: the type of customer, products and services, countries or geographical areas, type of transactions, delivery channels.

The business risk assessment must be documented and must be available to the relevant competent authority upon request. The business risk assessment must be reviewed and managed at regular, predefined intervals and it must be approved by senior management. See Appendix 5 for a template risk assessment.

## How the risk assessment affects customer due diligence

In deciding the level of Customer Due Diligence (CDD) to be applied, intermediaries, when undertaking a transaction/entering a business relationship, must consider a number of factors, including: the relevant business risk assessment, the purpose of an account/relationship, the level of assets deposited/the size of the transaction and the regularity of transactions/duration of the business relationship.

Legislation allows designated persons to apply aspects of the customer due diligence requirements on a risk-sensitive basis depending on:

a) The nature of the product being sold;
b) The delivery mechanism or distribution channel used to sell the product;
c) The profile of the customer; and
d) The customer's geographical location and source of funds.

The majority of focus is on risks from a product led perspective; however, there are situations where the delivery mechanism may add to the product risk. This is particularly the case with regard to non-face to face sales.

### (A) Product risk

The nature of the product being sold is usually the primary driver of the risk assessment. Characteristics such as where product features are defined and restricted; where the policy will only pay out on a verifiable event such as death or illness or where the policy is only accessible after years of contributions would mean that generally these types of products are standard. A small number of products such as single premium investment bonds do feature increased flexibility. This should be acknowledged in the application of the risk-based approach.

### (B) Distribution Risk (which may alter the risk profile)

#### "Face to Face" with no facility to take copies of ID

Where the interaction with the customer is on a face to face basis, the designated person should have sight of the original document(s) and appropriate details should be recorded. Where the customer is visited at his/her home address, the designated person should make a detailed record of the visit. This would include, for example, taking details of passport or driving license numbers.

Brokers Ireland recommends that in such scenarios, the customer is requested to forward a copy of the relevant ID and that it is cross referenced with the details which were recorded at the point of sale.

#### "Non-face to face"

The extent of the Customer Due Diligence in respect of non face-to-face customers will depend on the type of product or service requested and the assessed money laundering risk presented by the customer. Where the customer is not physically present (eg. by post, telephone or over the internet) for identification purposes, additional measures should be undertaken to establish the customer's identity. Examples of additional measures include:

- Telephone contact with the customer prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise) or a welcome call to the customer before the business relationship starts, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

- Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him which, in full or in part, may be required to be returned, completed or acknowledged without alteration);

- Verify information on documents received, for e.g. in relation to a utility bill forwarded; cross check against a bank statement narrative relating to entries from the utility bill provided or cross check salary details appearing on a recent bank or building society statement verifying the individual's employer as previously notified;

## Third Party Reliance

The primary responsibility for supervising intermediaries lies with the Central Bank of Ireland; however Product Providers, as a third party, retain responsibility for ensuring that Customer Due Diligence obligations have been met by the Intermediary. Product Providers are legally obliged, where an intermediary fails to meet the Customer Due Diligence requirements, to report this to the Central Bank of Ireland.

In order to comply with the Third Party Reliance requirements, Product Providers depending on their internal processes may require either:

1. Copies of all underlying documentary evidence from the intermediary for applicable products.

**or**

2. Confirmation of Verification of Identity where the Product Provider has the right of audit to ensure that the intermediary has the necessary documented evidence See Appendix 1.

## Customer Due Diligence (CDD)

CDD should comprise of the following:

**a)** Identifying the customer & verifying the customer's identity on the basis of documentation received.

**b)** Identifying, where applicable, the Beneficial owner* and taking adequate and risk based measures to verify his identity so that the designated person is satisfied as to the identity of the beneficial owner.

**c)** Obtaining information on the purpose and intended nature of the business relationship.

**d)** Conducting ongoing monitoring of the business relationship.

*Beneficial Owner is defined as any individual who ultimately owns or controls the customer and/or on whose behalf a transaction or activity is conducted.

Beneficial owner, in relation to a body corporate, is any individual who (other than a company having securities listed on a regulated market)

- ultimately owns or controls, whether through direct or indirect ownership or control (including through bearer shareholdings), more than 25 per cent of the shares or voting rights of the body; or
- otherwise exercises control over the management of the body.

Beneficial owner, in relation to a partnership, means any individual who

- ultimately is entitled to or controls, whether the entitlement or control is direct or indirect, more than a 25 per cent share of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership; or
- otherwise exercises control over the management of the partnership

There are three categories of Customer Due Diligence (CDD)

- **Simplified Customer Due Diligence** applies to low risk customers and product.
- **Enhanced Due Diligence** applies to High Risk Third Countries, Relationship/transaction presents higher risk & Politically Exposed Persons who are deemed to be high risk.
- **Standard Due Diligence** must be applied to all remaining customers and products.

In addition to the requirement under the 2010 Act that customer due diligence be carried out at particular times, the 2018 Act adds that CDD must be executed at any time, including situations where the relevant circumstances of a customer have changed, where the risk of money laundering/terrorist financing warrants its application.

The firm is required to review and update the firm's documented customer due diligence procedure to ensure that: It comprehensively details the Firm's obligations as a designated person in its own right reflective of current AML/CFT legislative and regulatory requirements; and it reflects the customer due diligence the Firm undertakes in practice.

## 1. Simplified Customer Due Diligence (SCDD)

Designated persons will be allowed to carry out SDD where the customer or business area is considered to be low risk. SDD can only be applied where a designated person has identified in its business risk assessment, an area of lower risk into which the relationship or transaction falls, and the relationship or transaction concerned can reasonably be considered to be low risk. Please see Appendix 7 and Appendix 8 for a list of factors suggesting potentially lower and higher risk.

Where this section is applied, the reasons for its application and the evidence on which it was based must be recorded and the business relationship and transactions must be monitored to enable the designated person to detect unusual or suspicious transactions.

Simplified Customer Due Diligence (SCDD) means that a designated person does not need to comply with the CDD obligations as listed in the paragraph a-c as mentioned above. The designated person must obtain sufficient information about the customer to satisfy that the customer meets the criteria for Simplified Due Diligence. Simplified Due Diligence applies to the following insurance "specified products":

- Life assurance policy having an annual premium of no more than €1,000 or a single premium of no more than €2,500.
- Pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral (e.g. Pension Term Assurance).

**Important:** There is no exemption from the obligation to verify identity where there is a suspicion that a transaction involves money laundering or terrorist financing or where there is doubt about the veracity or accuracy of documents previously obtained from the client.

## 2. Enhanced Due Diligence (EDD)

1) High risk third countries
   A designated person is required to apply enhanced customer due diligence measures when dealing with a customer established or residing in a high-risk third country. There is an exemption that applies when the customer is a branch or majority-owned subsidiary of a designated person established in the European Union which complies with the group's group-wide policies and procedures. These cases must be dealt with using a risk-based approach.

2) Relationship/transaction presents a higher risk
   A designated person is required to apply enhanced customer due diligence measures where a business relationship or transaction presents a higher degree of risk. This is to be applied where the relationship or transaction concerned can reasonably be considered, having regard to certain matters, to be high risk.

3) Politically Exposed Persons (PEPs)

Enhanced Due diligence measures that previously applied only to PEPs resident outside of Ireland now also apply to PEPs resident in Ireland.
"PEP" is an individual who has been entrusted with prominent public functions or an immediate family member or a known close associate of such a person.

Life Assurance Policies/PEPs
Additional requirements are imposed regarding the identification of the beneficiaries of life assurance policies and other investment-related assurance policies. Specific steps must be taken where the PEP is a beneficiary of a life assurance policy. If a designated person knows or has reasonable grounds to believe that a beneficiary of a life assurance or other investment-related assurance policy or a beneficial owner of the beneficiary concerned, is a politically exposed person, or an immediate family member or a close associate of a politically exposed person, it shall:

a) inform senior management before pay-out of policy proceeds and
b) conduct enhanced scrutiny of the business relationship with the policyholder

The firm must outline what process it has in place to demonstrate how it is meeting its obligations as to how it assesses it's customer base to determine whether a customer is /has become a PEP or is an immediate family member, or close associate, of a PEP at onboarding and during the course of the business relationship.

The domestic insurance sector has a very low exposure to Politically Exposed Persons. Also, the majority of products sold by insurers do not lend themselves to moving the proceeds of corruption. Therefore, it is likely that the number of customers meeting the high-risk criteria is very low and those that are identified as PEPs is lower still.

Designated persons must have processes in place prior to establishing a business relationship with a customer to determine whether the person may be deemed a "PEP". In practice, designated persons should take steps to establish whether the person is deemed to be politically exposed. The identification of a customer as a PEP is not in itself cause for suspicion, but does requires an enhanced level of due diligence. See Appendix 2

## 3. Standard Due Diligence (SDD)

There are 3 overall levels of risk for insurance products, these are:

- Low risk;
- Intermediate risk; or
- Increased risk.

### Low risk

Products due to their inherent features are unlikely to be used as a vehicle for money laundering purposes. The following table shows the type of product and the product features which would qualify them as a low risk level.

| Protection/Pension | Typical Features |
|---|---|
| 1 Term life assurance | ▪ Only pays out on death of policy holder<br>▪ No surrender value<br>▪ Small, regular premiums: additional payments by customer not possible<br>▪ Large premiums will normally require medical evidence<br>▪ No investment element |

| | |
|---|---|
| | ▪ Once the term of policy is finished there is no payout and policy ceases |
| 2 Income protection products related to long-term illness | ▪ Only pays out on medical evidence and proof required as to loss of income<br>▪ No surrender value<br>▪ Small, regular premiums: additional payments by customer are not possible |
| 3 Critical illness products relating to diagnosis of a specific critical illness | ▪ Only pays out on medical evidence<br>▪ No surrender value<br>▪ Small, regular premiums: additional payments by customer are not possible |
| 4 Whole of Life | ▪ May accrue some small surrender value<br>▪ Benefits usually payable on death or diagnosis of terminal illness or in some cases, critical illness of the policyholder<br>▪ Partial surrenders are normally allowed within specified limits |

- Generally, for protection products, due diligence requirements is satisfied by the information collected on the application form in conjuction with the fact that the payment is made from an account in the customer's name (ie. personal cheques and other payment instruments drawn on a customer's account such as Direct Debits/Standing Orders)

- If payment is made by bank draft for the products above Brokers Ireland would recommend that the client is requested to request confirmation from the bank confirming where the money is coming from.

### Medium Risk

The medium risk level is given to products whose inherent features pose some risk for the purposes of money laundering or terrorist financing. These may be products which have a facility for "top up" payments.

| Savings | Typical features |
|---|---|
| Life assurance savings plan (unless premium is less than €1,000 AP or €2,500 SP, then Simplified Customer Due Diligence can apply). | ▪ Long term savings plan often for retirement<br>▪ Requires at least five years to gain positive return on investment<br>▪ Often unable to be surrendered in first or second year, with penalties in years three to five<br>▪ Additional 'top up' payments may be permitted |
| **Endowments** | ▪ Long term savings plan for a set term(were often linked to mortgages)<br>▪ Usually long term, 10-25 years |

The recommended standard for intermediate risk is as follows (subject to exemptions): Verify the identity of the customer and/or the relevant parties at the outset of the business relationship.

- Due diligence requirements is satisfied by the information collected on the application form in conjuction with the fact that the payment is made from an account in the customer's name (ie. personal cheques and other payment instruments drawn on a customer's account such as Direct Debits/Standing Orders)

- If payment is made by bank draft for the products above Brokers Ireland would recommend that the client is requested to seek confirmation from the bank of where the money is coming from.

### High Risk

This level of risk has been given to products whose inherent features allow for the possibility of being used for money laundering purposes. These products have the facility for third party and/or "top up" payments and therefore an enhanced level of due diligence (by asking for more information) is appropriate. It is to this risk level that the majority of a designated person's AML resource will normally be directed. The majority of products in this range are found in the investment category which reflects the higher value premium that can be paid into them.

| **Protection** | |
|---|---|
| None | |
| **Savings and Investments** | **Typical features** |
| Single premium investment bonds, including:<br>▪ With profits<br>▪ Guaranteed<br>▪ Income<br>▪ Investment<br>▪ Offshore international bonds | ▪ Open ended investment<br>▪ Usually a 5 year recommended<br>▪ minimum investment term but can be surrendered earlier<br>▪ Additional 'top up' payments permitted by the policy holder and by third parties<br>▪ May be segmented and individual segments may be assignable |

The recommended industry standard for increased risk products is as follows:

1. Verify the identity of the customer and/or the relevant parties as per the "One plus One" approach of one item from the list of photographic IDs (to verify name and date of birth) and one item from list of non-photographic IDs (to verify address) at the outset of the business relationship

   Sources which can be used to verify identity are:

   - Current valid Passport
   - Current valid driving licence
   - Current valid National Identity Card
   - In the absence of the above documents, written or otherwise documented assurances from persons or organisations that have dealt with the customer for some time may suffice.

   Non-photographic IDs

   - Current official documentation/cards issued by the Revenue Commissioners and addressed to the individual;
   - Current official documentation/cards issued by the Department of Social and Family Affairs and addressed to the individual;
   - Instrument of a court appointment (such as liquidator or grant of probate);
   - Current local authority document e.g. refuse collection bill, water charges bill (including those printed from the internet);
   - Current statement of account from a credit or financial institution, or credit/debit card statements (including those printed from the internet);

- Current utility bills (including those printed from the internet);
- Current household/motor insurance certificate and renewal notice;

In cases where a plausible explanation is offered by a customer as to why the above non photographic documentation cannot be provided, the following may be used to assist in confirming the identity of the customer, having regard to any data protection requirements:

- Examination of the electoral register (including online version)
- Examination of a local telephone directory or available street directory;
- Confirmation of identity by a known/recognisable employer;
- Search of a relevant agency that can confirm identity.

The above identification and verification procedures may usefully be supplemented (on a risk basis to be decided by the designated person) by media searches and use of internet search engines.

Copies of proof of identity and address should be marked original sighted, dated and signed.

**AND**

2. Acquire prescribed information at the outset of the business relationship to satisfy the additional suggested information requirements:
   **a)** Source of funds for the transaction e.g. an Irish bank account in own name.
   **b)** Employment and salary details - this information could be captured in the Factfind.
   **c)** Source of wealth (e.g. inheritance, divorce settlement, property sale). This information should be captured on the source of wealth form. See Appendix 3

### Monitoring

Designated persons should undertake monitoring on an ongoing basis for patterns of unusual or suspicious activity to ensure that higher risk activity is scrutinised. "Complex or unusually large" transactions, or "unusual patterns of transactions" must be investigated in greater detail and monitoring increased if they appear suspicious.

Monitoring means the scrutinising of transactions, and the source of wealth or of funds for those transactions, undertaken during the relationship in order to determine if the transactions are consistent with the designated person's knowledge of—

a) the customer,
b) the customer's business and pattern of transactions, and
c) the customer's risk profile (as determined under section 30B), and

ensuring that documents, data and information on customers are kept up to date in accordance with its internal policies, controls and procedures

In practice, this might occur where there is an early surrender of a policy, encashment requests or where the payer of the policy changes. Employees should be adequately trained to identify such unusual business and report to the designated person's MLRO. For example, where an encashment request is received, the intermediaries' procedure may be to take additional measures to ensure the request is genuine such as:

- ✓ Phone the client to confirm the details/instruction
- ✓ Cross reference proof of ID and residency with existing proof of identity and residency on file

The key consideration when taking measures to prevent terrorist is to examine the intended use or destination of the funds as opposed to its origin.

### Management Responsibilities

The Central Bank recommends that the topic of AML/CTF is a recurring agenda item at board/senior management/ownership level meetings. The firm must ensure that AML/CFT/FS issues and decision making in relation to AML/CFT/FS is evidenced in the firm's board/management meeting minutes.

### Procedures/Policies

Designated persons are obliged to ensure that they comply with the requirements of the Criminal Justice (Money Laundering and Terrorist Financing) Acts. Procedures should be compliant with the Central Bank's core and sectoral guidance notes. See Appendix 4

The firm must ensure that the AML/CFT/FS policy and procedure reflects the practices within the firm and the policy and procedures should be reviewed at least on an annual basis. The firm must have a documented wide risk assessment in place which demonstrates consideration of risk pertaining to the firms products/services, customer base, jurisdictions and distribution channel.

Firms must adopt internal policies, controls and procedures in relation to their business to prevent and detect the commission of money laundering and terrorist financing. These requirements also apply to persons to whom AML obligations have been outsourced.

The internal policies, controls and procedures are to include:

(a) identification, assessment, mitigation and management of risk factors relating to money laundering/terror financing
(b) customer due diligence measures
(c) monitoring transactions and business relationships
(d) the identification and scrutiny of complex/large transactions, unusual patterns of transactions and any other activity that the designated person has reasonable grounds to regard as particularly likely to be related to money laundering/terrorist financing
(e) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,
(f) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments,
(g) reporting (including the reporting of suspicious transactions),
(h) record keeping,
(i) measures to be taken to keep documents and information relating to the customers of that designated person up to date,
(j) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,
(k) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and
(l) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures.

Documents and other records relating to clients shall be kept for a period of not less than five years.

Policies, controls and procedures must be approved by senior management and these should be kept under review in particular when there are changes to the business profile or risk profile of the firm. These policies, controls and procedures are to have regard to any guidelines issued by the competent authority.

Firms must ensure that persons involved in the conduct of the business (this includes directors, other officers and employees) receive instruction and training in respect of the law and on how to identify

transactions or other activity that may relate to money laundering or terrorist financing (suspicious transactions) and how to proceed once identified.

### Record Keeping

Designated persons are required to keep records evidencing the procedures applied and the information obtained, when carrying out CDD on customers for a period of at least 5 years after the business relationship with their customer has ended. Record keeping is an essential part of the evidence trail and sufficient processes must be put in place to ensure that records are adequately kept.

Records that must be kept:

- Customer information collected to comply with the requirements of Legislation; and
- Information regarding transactions undertaken by customers.
- Possible formats in which records can be retained include one or more of the following:
- Original documents
- Photocopies of original documents
- On microfiche
- In scanned form
- In computerised or electronic form

These records may be kept wholly or partly in electronic form only if they are capable of being reproduced in a written form. All records should be capable of being reproduced in the State as per Legislation for a period not less than 5 years.

### Requests from An Garda Síochána for client information/records

For the purposes of providing information to the Garda Síochána this must be requested in writing be a member of the force not below the rank of Sergeant (who may give a direction, which must also be in writing, to retain the documents/other related records for a period up to a maximum of five years.

### Staff Training

All staff, including directors and other officers such as MLROs must receive regular training in relation to their AML and combating of terrorist financing obligations. Failure by the employer to provide training is an offence under the requirements. Employers must therefore retain evidence of training provided.

It is recommended that annual anti-money laundering training be provided to staff on an annual basis. The content of the firms training must be consistent with legislative and regulatory requirements and be tailored to the firm's business activities and consistent with firm policy and procedures document. The Firm must review and consider their AML/CFT/FS training process and ensure that all staff receive appropriately tailored AML/CFT/FS training on an annual basis.

The Firm must review and consider their AML/CFT training process and ensure that the Firm's MLRO can demonstrate annual attendance at AML/CFT/FS training appropriate to his/her role as MLRO.

It must be demonstrated that any new employees (where relevant) receive AML/CTF/FS training and there is evidence that this training took place.

Directors need to be trained too to understand their oversight and governance obligations. Includes non-exec directors.

Details in relation to staff training should be retained for a period of 5 years.

## Reporting

A report must be made when there is knowledge or suspicion or reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted.

The firm should put in place an internal reporting process, it should document the process for staff to report suspicious transaction reports. There should be documented timelines in relation to the filing of the Suspicious Transaction Reports.

All reports submitted via the internal reporting process should be recorded. This report should include appropriate details of the customer who is the subject of concern and a statement containing as much of the information giving rise to the knowledge or suspicion, as possible. The Money Laundering Reporting Officer (MLRO) will then decide whether to make the firm's report to the Garda Bureau of Fraud Investigation and the Revenue Commissioners. If the MLRO decides not to make an external report, the reasons for not doing so should be recorded and retained.

If the MLRO decides to make an external report, it must be made to the FIU via the GoAML system and the Revenue Commissioners. The following information should be contained in the report:

a) The information on which the designated person's knowledge, suspicion or reasonable grounds are based;
b) The identity of the suspected person;
c) The whereabouts of the property that is the subject of the money laundering or the funds that are the subject of the terrorist financing;
d) Any other relevant information.

Under the Legislation, it is an offence to disclose to the customer concerned or other third persons that a report has been made to the Gardaí/FIU/Revenue Commissioners in relation to suspicions of money laundering or terrorist financing.

## Financial Sanctions

Financial sanctions are restrictive measures imposed on individuals or entities in an effort to curtail their activities and to exert pressure and influence on them. These restrictive measures include, but are not limited to, financial sanctions, trade sanctions, restrictions on travel or civil aviation. These are imposed by both the EU and the UN. The obligations which are imposed by the EU and UN do not fall within the AML/CTF legislation but exist side by side with it.

The firm must demonstrate that it has fully considered its obligations in respect of Financial Sanctions and that it has appropriate procedures in place to undertake reviews of the firm's customer base against the Financial Sanctions lists.

It is necessary for firms to monitor their customers and transactions against both the EU and UN Sanctions Committees lists relating to terrorism. Financial Sanctions lists that relate to terrorism should be monitored to assist in preventing terrorist financing from occurring, including, but not limited to, the following:

- EU Financial Sanctions list
- United Nations Sanctions Committees lists

The firm must ensure that their documented procedure for Financial Sanctions is reflective of what the firm actually does in practice. The procedure should outline how, when and by whom the firm's customers are screened against Financial Sanctions lists at on-boarding and an ongoing basis, the

process for investigation after a match is made. The process for discounting a match or the process whereby the MLRO decides to report a Financial Sanction match to the Central Bank should be documented. Intermediaries should check with their CRM providers to confirm if the facility to run these checks is available on their systems.

### What to do if a customer is on a terrorist list

If you have knowledge or a suspicion of terrorist financing, a suspicious transaction report must be sent to An Garda Síochána and the Revenue Commissioners.

If a customer is matched to either the EU or UN terrorist lists, a report should be filed of a suspicious transaction immediately with the FIU in the Garda Bureau of Fraud Investigation and not carry out any service or transaction until the report has been made. When the report is made, the Gardaí can take steps and/or give directions in respect of the account. Where a person or entity is listed in an EU Council Regulation relating to terrorism, there is a legal obligation to immediately freeze that person or entity's account.

### Role of the Money Laundering Reporting Officer

The role of Head of Compliance with responsibility for AML/CTF legislation is a pre-approval controlled function in the context of the Central Bank Reform Act 2010. The MLRO has the role of ensuring communication of reports of suspicious transactions to the FIU and the Revenue Commissioners and acts as a liaison between the Intermediary and the FIU and the Revenue Commissioners. However, section 41 of the Act makes clear that the requirement for designated persons to report suspicious transactions extends to any person acting 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.

The MLRO has a significant degree of responsibility and should be familiar with relevant aspects of the Act and these guidelines. He/she is required to determine whether the information or other matters contained in the suspicious transaction he/she has received via any internal reporting procedure merit the making of a report to the FIU and the Revenue Commissioners.

A formal register should be maintained by the MLRO of all suspicious transactions reports, the determinations made, any subsequent reports made to the FIU and the Revenue Commissioners and any further correspondence sent or received. Where the MLRO decides not to make a report to the FIU and Revenue Commissioners, a record of that fact should be recorded together with the reason/s for not making the report.

The MLRO should provide the board at least on an annual basis an AML/CTF/FS report.

### Central Bank

The Central Bank of Ireland is deemed to be the competent authority responsible for monitoring compliance of designated persons with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended 2018. The Central Bank has the power under the Administrative Sanctions Regime to sanction for failure to comply with the necessary obligations.

CERTIFICATION OF IDENTIFICATION PROCEDURES TO COMPLY WITH THE MONEY LAUNDERING PROVISIONS OF the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

[To be produced on intermediary's headed notepaper.]

I, _____(name), of _____(name of firm) confirm that the Customer Due Diligence procedures have been completed in accordance with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 in respect of the following client and that a copy of the identification material will be furnished to _____( Insurer) on request.

Signature of /on behalf of (intermediary) _____

Name of client_____

Address_____
_____
_____
_____

Policy/Proposal Number_____

Occupation/Nature of Business_____

**Detail below the CDD measures undertaken in relation to the client (Include details of documents etc used to verify identity)**

PROCEDURE TO COMPLY WITH THE MONEY LAUNDERING PROVISIONS OF [THE THIRD MONEY LAUNDERING DIRECTIVE] IN RELATION TO POLITICALLY EXPOSED PERSONS

[To be produced on intermediary's headed notepaper.]

**Politically Exposed Person (PEP)**

A "PEP" is defined as a person who is, or has at any time in the preceding 12 months been, entrusted with prominent public function, this includes

- Heads of State, heads of government, ministers and deputy of assistant ministers.
- Members of Parliament
- Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.
- Members of courts of auditors or the board of central banks
- Ambassadors, charges d'affaires and high ranking officers in the armed forces
- Members of the administrative, management or supervisory boards of state owned enterprises
- A Family member/close associate of one of the above

**Customer Declaration**

I have read and understand the above definition of a Politically Exposed Person and confirm that:

I am not a Politically Exposed Person ☐

I am a Politically Exposed Person ☐

Signed: Dated: / /

To comply with the current Anti Money laundering and Terrorist Financing legislation, we are required to ask you about the original source of your wealth in respect of this application. Please tick the relevant box and indicate how the amount available for **this** investment is made up.

| **Source of Wealth** | **Please tick as appropriate** |
|---|---|
| 1. Salary, bonus or regular savings | ☐ |
| 2. Early retirement or redundancy payment | ☐ |
| 3. Proceeds from the sale of investments (including proceeds from Life assurance plan) or other assets | ☐ |
| 4. Inheritance | ☐ |
| 5. Windfall/compensation payments | ☐ |
| 6. Other (please specify) | ☐ |
| Total | |

DECLARATION OF COMPLIANCE WITH THE MONEY LAUNDERING PROVISIONS OF THE MONEY LAUNDERING PROVISIONS OF the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010.

[To be produced on intermediary's headed notepaper and retained with the Brokers Ireland guidance notes.]

I_____ of _____ confirm that the firm complies with procedures and internal policies to comply with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended 2018.

Signed: Date:

## Anti-Money Laundering & Counter Terrorist Financing Risk Assessment of ABC Ltd for 20xx

**IMPORTANT:** This document is for guidance purposes only and members must ensure that a comprehensive Anti-Money Laundering & Counter Terrorist Financing (AML/CTF) Risk Assessment has been undertaken by senior management which demonstrates that all potential AML/CTF risks pertinent to their business have been fully considered and challenged. This risk assessment must be documented.

This risk assessment **must be personalised** by the firm to reflect their business and should be completed on an annual basis, it should detail such information as how the firm assesses its AML/CTF risk, time dedicated to it within the firm, review of transactions etc.

**Executive Summary**

- Confirm Brokerage's name, address and legal status
- Detail current Authorised status: IIA, IMD, CCA and CMCAR
- Confirm how many years the entity has been trading and the current number of clients
- Name of senior management/sole trader/partner who has oversight of the AML/CTF functions at the firm

**How does the firm assess the AML/CTF risks it faces?**

**a) The nature of the products being sold in the firm**

Provide an analysis of products/services provided by the firm. Detail the percentage of the firm's regulated services:
Protection - %
Pensions - %
Investment - %
Savings - %
Mortgages - %

*"The nature of the product being sold is usually the primary driver of the risk assessment in small brokerages. Characteristics such as where product features are defined and restricted or where the policy will only pay out on a verifiable event such as death or illness would mean that generally these types of products are standard."*

Does the firm anticipate an increase in business from high[1] risk products? If so detail here:

_____

**Risk Assessment Sheet**

| Product Name | Product AML CTF | No. of Customers | No. of Customers | No. of Customer | No. of Customers | No. of PEPs |
|---|---|---|---|---|---|---|

[1] This level of risk would be given to products whose inherent features allow for the possibility of being used for money laundering purposes. These products have the facility for third party and/or "top up" payments and therefore an enhanced level of due diligence is appropriate. It is to this risk level that the majority of a firm's AML resources will normally be directed. The majority of products in this range are found in the investment category which reflects the higher value premium that can be paid into them. A small number of products such as single premium investment bonds do feature increased flexibility". This should be acknowledged in the application of the risk-based approach.

| | risk rating | | rated High Risk (excluding PEPS) | rated Medium Risk | rated Low Risk | |
|---|---|---|---|---|---|---|
| ABC Product | Low | | | | | |
| XYZ Product | High | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

b) **The delivery mechanism or distribution channel used to sell the product**

Provide a breakdown of sales carried out - detail whether the firm conducts its services mainly on a "face-to-face" basis or "non-face-to-face basis".

Detail here if the firm anticipates that there will be an increase in non-face-to-face business completed next year?

Would the firm automatically treat a non-face-to-face transaction as a higher risk or would the extent of the Customer Due Diligence in respect of non-face-to-face customers depend on the type of product or service requested and the assessed money laundering risk presented by the customer?

Detail what additional measures of customer due diligence would be undertaken in respect of non-face-to-face clients.

Examples:

- *Telephone contact with the customer prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise) or a welcome call to the customer before the business relationship starts, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;*
- *Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him which, in full or in part, may be required to be returned, completed or acknowledged without alteration);*
- *Verify information on documents received, for e.g. in relation to a utility bill forwarded; cross check against a bank statement narrative relating to entries from the utility bill provided or cross check salary details appearing on a recent bank or building society statement verifying the individual's employer as previously notified*

**c) The profile of the customer**

Provide an analysis of the firm's customer base:

Outline whether the firm's client base will be individual and/or corporates and what percentage of both.
Individuals xx%
Corporates xx%
Do you expect there to be a change in the customer profile of the firm which may lead to potential AML/CTF risks?
Yes ☐
No ☐

If yes, detail what procedures the firm implemented to mitigate this risk?

**d) The customer's geographical location and source of funds**

Confirm general geographical location of clients

Provide an assessment of the jurisdictions the firm operates in, including the jurisdiction in which your clients are resident and if your firm is "passporting" its services.

Does your firm anticipate an increase in this risk ((e.g. customers moving to high risk jurisdictions) and what measure are in place to manage and mitigate this risk?

Does the firm have policies and procedures to adequately define or outline the requirements to satisfy Source of Funds? For example, does the firm consider the risk of potential 3rd party payment when accepting a bank draft and what procedures are in place to mitigate against such risk.

**Risk Assessment Completed by: _____**
**Dated: _____**

## Appendix 6

## EXPECTATIONS OF THE CENTRAL BANK ON NON-LIFE INTERMEDIARIES

What is the Offence of Money Laundering?

The process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities constitutes the offence of Money Laundering. If undertaken successfully, money laundering enables criminals to legitimise "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of income. A person who knows or believes (or is reckless as to whether or not) the property is the proceeds of criminal conduct, is also guilty of an offence.

### What is Money Laundering?

The following conduct shall be regarded as money laundering:

- Engaging in any of the following acts in relation to property that is the proceeds of criminal conduct:
    1. Concealing or disguising the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;
    2. Converting, transferring, handling, acquiring, possessing, or using the property;
    3. Removing the property form, or bringing the property into, the State.

### What is expected of non-life intermediaries?

General insurance intermediaries have to put in place systems and controls to prevent financial crime, which includes money laundering. Failure to have adequate systems and controls in place, for example, the absence of a process for reporting knowledge or suspicions of money laundering, put these firms and their employees at risk of committing money laundering offences. Many firms therefore choose to implement controls similar to those adopted by firms who are subject to the Money Laundering legislation.

### Guidance for Staff – Reasonable Grounds for Knowledge or Suspicion;

It is important that intermediaries do not turn a blind eye to information, but make reasonable enquiries. A healthy level of professional scepticism should be maintained, if in doubt you should err on the side of caution and make a report to the appropriate internal reporting processes i.e. to the Money Laundering reporting Officer.

As part of our CDD process, intermediaries must identify and scrutinise large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose, and any other activity that we have reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing. We should be in a position to demonstrate compliance with this requirement. It is recommended that the background and purpose of such transactions should, as far as possible, be examined and the findings established in writing.

### Examples of attempted Money Laundering

- Premium payments being made by 3rd Parties
- More than one large claim, or unusual pattern or frequency of claims
- Requests for claim payments to be made to 3rd Parties
- More than one cancellation of insurance which results in substantial refunds due, and/or requests for such refunds to be made to 3rd Parties
- Small business with a massive turnover e.g. 10 times more than would be expected e.g. a small café.

Not all of the above means that there is attempted money laundering however if there is a suspicion you must report this to the Money Laundering Reporting Officer (MLRO).

The MLRO will undertake an investigation into the matter and will make a decision to report to An Garda Siochana or the Revenue Commissioners. If the MLRO decides onward reporting is not warranted, i.e. the MLRO believes the investigated activities are not suspicious or do not constitute money laundering, then he must evidence his investigation and why reporting is not warranted. However, if after investigation there is a suspicion that money laundering or other financial crime is taking place, it must be reported to an Garda Siochana and/or Revenue Commissioners.

### Reporting Procedures

The nominated MLRO is charged with responsibility for reporting money laundering suspicions to the Gardaí and the Revenue Commissioners.

Where you know, suspect, or have reasonable grounds to suspect that another person has been or is engaged in an offence of money laundering or terrorist financing, the formation of such a suspicion triggers a reporting duty which is absolute.

It is an offence not to report suspicious transactions (fine and/or imprisonment).

It is also an offence to advise the other person that you have reported suspicions about them to the MLRO or Garda Siochana (fine and/or imprisonment).

All such reporting (and persons who made the report) are protected by legislation (Whistleblowing).

*Non exhaustive List of factors considered potentially* ***lower risk***

Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
(b) public administrations or enterprises;
(c) customers that are resident in geographical areas of lower risk as set out in subparagraph (3).

Product, service, transaction or delivery channel risk factors:

(a) life assurance policies for which the premium is low;
(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

Geographical risk factors:

(a) Member States;
(b) third countries having effective anti-money laundering (AML) or combating financing of terrorism (CFT) systems;
(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised Financial Action Task Force (FATF) recommendations and effectively implement these requirements.".

*Non-exhaustive list of factors suggesting potentially* ***higher risk***

Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;
(b) customers that are resident in geographical areas of higher risk as set out in subparagraph (3);
(c) non-resident customers;
(d) legal persons or arrangements that are personal asset-holding vehicles;
(e) companies that have nominee shareholders or shares in bearer form;
(f) businesses that are cash intensive;
(g) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

Product, service, transaction or delivery channel risk factors:

(a) private banking;
(b) products or transactions that might favour anonymity;
(c) non-face-to-face business relationships or transactions;
(d) payment received from unknown or unassociated third parties;
(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Geographical risk factors:

(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
(c) countries subject to sanctions, embargos or similar measures issued by organisations such as, for example, the European Union or the United Nations;
(d) countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.".