Brokers Ireland Guidance on the

Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

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

and

The Central Bank of Ireland's Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector 2019

OCTOBER 2020

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 1.

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 an occasional transaction or service for a customer;
- prior to carrying out any service for a customer, if, having regard to the circumstances, the firm has reasonable grounds to suspect that the customer is involved in, or the service, transaction or product sought by the customer is for the purpose of ML/TF;
- prior to carrying out any service for a customer where the firm has reasonable grounds to doubt the veracity or adequacy of documents; and
- at any time, including where the relevant circumstances of a customer have changed

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 the customer. 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: i) name, legal form and proof of existence; ii) the powers that bind and regulate the legal person or arrangement; iii) the address of the registered office (where applicable) and main place of business; and iv) the nature of the business and its ownership	This could generally be satisfied by either ✓ 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 ✓ 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. ✓ 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 ✓ 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 ✓ relevant and up-to-date legal opinion from a reliable source documenting due diligence conducted, including in relation to information on

			directors; or ✓ obtaining information from relevant company or another registry such as the CRO or known foreign equivalent; or ✓ 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.

A business risk assessment should consist of two distinct but related steps:

- Identifying ML and TF risks relevant to a Firm's business; and
- Assessing the identified ML and TF risks in order to understand how to mitigate those risks.

Firms should rely on their assessment of the risks inherent in their business to inform their risk-based approach to the identification and verification of an individual customer. This in turn should drive the level and extent of due diligence appropriate to that customer. A business risk assessment will assist firms to understand where they are exposed and which areas, they should prioritise to combat ML/TF.

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. When drafting and carrying out a business risk assessment, firms should use various sources, such as

- Communications issued by FIU Ireland;
- Risk Factors contained in Schedule 3 and 4 of the CJA 2010;
- Guidance, circulars and other communication from the Central Bank and other relevant regulatory bodies;
- Information from industry bodies;
- EU Measures, including financial sanctions and designation of high-risk countries;

- Information from international institutions and standard setting bodies relevant to ML/TF risks (e.g. UN, IMF, Basel, FATF); and
- Other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by a firm on a risk-sensitive basis.

The business risk assessment must be documented and must be available to the relevant competent authority upon request. Where a firm decides to apply a different standard of CDD measures in circumstances where it believes, following a risk assessment, that a lower level of ML/TF risk applies, the firm should document its rationale for this. This should assist a firm in demonstrating to the Bank that is has complied with its obligations under the CJA2010 and CJA2018(as amended).

Firms should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business risk assessments. Accompanying customer due diligence measures should also be amended accordingly.

The business risk assessment must be reviewed and managed at regular, predefined intervals and it must be approved by Senior Management (or equivalent*). See Appendix 2 for a template business risk assessment. In addition, Senior Management must review and approve the methodology used for undertaking the firm's business risk assessment.

Systems and controls should be put in place to ensure the individual and business risk assessments remain up to date. Examples include: Setting a timeline on which the next risk assessment update will take place, to ensure changing, new or emerging risks are included in risk assessments. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible;

Carefully recording issues throughout the year that could have a bearing on risk assessments, such as:

- Internal suspicious transaction reports;
- Compliance failures and intelligence from front office staff; or
- Any findings from internal/external audit reports;

Like the original risk assessments, any update to a risk assessment and adjustment of accompanying CDD measures should be documented, proportionate and commensurate to the ML/TF risk.

Firms should consider the outcomes of their own business risk assessments and whether the frequency and content of AML/CFT training provided is adequate for levels of ML/TF risks faced by the firm.

Firms should also ensure the business risk assessment takes into account their obligations under financial sanctions regulations.

*Or equivalent means in the case of a Sole Trader/One director companies/Partner of the business, its Principal.

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. The risks to be considered would include the level of transparency the product affords, the complexity of the product, and its value or size. 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. The firm's business risk assessment should be updated to capture any risks relating to new products.

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

The risks to be considered would include the extent that the business relationship is conducted on a non-face to face basis, and any introducers or intermediaries the business may use and the nature of their relationship with the firm.

"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*

*In practice, providers require copies of the underlying documentary evidence.

(C) Customer Risk

In order to assess the level of customer due diligence to be applied, firms must identify and assess the ML/TF risk in relation to a customer or particular transaction. The risks to be considered would include the customer's and their beneficial owner's business or professional activity, their reputation and their nature and behaviour.

(D) Country or Geographical Risk

The level of risk, and therefore the level of due diligence to be applied depends on the jurisdiction in which the customer and its beneficial owners are based, where their main place of business is located, and whether they are within the EU or in a Third Country.

Customer Due Diligence (CDD)

In determining the level of due diligence to be applied, firms should take into account the relevant business risk assessment, the purpose of the relationship, the size of the transaction, and any risk factors contained within Appendices 4 and 5. The firm is to document their rationale for choosing the level of due diligence, and retain their rationale in accordance with their policies and procedures. Before the establishment of the business relationship, or the carrying out of the first

transaction, firms are required to identify and verify customers and where applicable beneficial owners.

CDD involves more than just verifying the identity of a customer. Firms should collect and assess all relevant information in order to ensure that the firm:

- Knows its customers, persons purporting to act on behalf of customers and their beneficial owners, where applicable;
- Knows what it should expect from doing business with them; and
- Is alert to any potential ML/TF risks arising from the relationship.

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

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

- ultimately is any individual who is entitled to a vested interest in the trust property may be considered a beneficial owner. Additionally, settlors, trustees and protectors of a trust may now also be considered beneficial owners. The threshold of 25 per cent ownership no longer applies.

Therefore, firms must identify all beneficial owners, where applicable, and verify the identity of the beneficial owners and the procedures to be applied in these circumstances.

There are three categories of customer due diligence (CDD)

- **Simplified 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.
- **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.

A client risk assessment form is recommended to be completed to assess the risk per transaction – See Appendix 3

1. Simplified Due Diligence (SDD)

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 4 and Appendix 5 for a list of factors suggesting potentially lower and higher risk. Prior to applying SDD measures, firms are required to conduct appropriate testing to satisfy themselves that the customer, business relationship or transaction qualifies for the simplified measures.

Examples of products which may fall into the simplified customer due diligence category are:

- Protection Policies with annual premium of less than €1000
- Pension Business (except ARF and AMRF)

Note: Intermediaries must at all times take into account the type of customer, countries or geographical areas, transactions and delivery channels and document the rationale for categorising these products as lower risk for the purposes of applying CDD.

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.

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)

In circumstances in which a firm has determined that a customer or business scenario presents a higher ML/TF risk, EDD measures should be applied. For example, has adequate information been obtained? If not, firms should seek additional documentation which may include establishing a customer's source of wealth/source of funds. EDD measures cannot be substituted for CDD measures but must be applied in addition to them.

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/transactions which present a higher risk

3) Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function. Many PEPs hold positions of influence and as a result carry a greater risk, if their influence is abused for the purpose of money laundering, corruption or bribery. In addition to that, any close business associates or family member of these people may also be deemed as being a risk and therefore could also be added to the PEP list.

Enhanced due diligence measures that previously applied only to PEPs resident outside of Ireland now also apply to PEPs resident in Ireland. Examples of PEPs are:

- Senior official of a major political party
- Senior official in the executive, legislative, administrative, military, or judicial branch of a government
- Senior executive of a government owned commercial enterprise or corporation.
- Any individual known to be a personal or professional associate of a PEP
- An immediate family member of a PEP; e.g. spouse, parents, siblings, children.

Firms should note that PEP status itself is intended to apply higher vigilance to certain individuals and put those individuals that are customers or beneficial owners into a higher risk category. It is not intended to suggest that such individuals are involved in suspicious activity.

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 or its equivalent 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 6

Firms should put appropriate policies and procedures in place to determine:

- if a customer or beneficiary is a PEP at onboarding or
- if a customer becomes a PEP during the course of the business relationship with the firm.

Firms should note that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship with the firm. On this basis, firms should undertake regular and on-going screening of their customer base and the

customers' beneficial owners (where relevant), to ensure that they have identified all PEPs. The frequency of PEP screening should be determined by the firm's approach documented with their business wide risk assessment.

3. Standard Due Diligence (SDD)

The purpose of the following section is to give guidance to members on how to apply CDD measures taking into account the product characteristics. Members are required to take into account all risk factors relating to their customers, countries or geographical areas, products and services, transactions and delivery channels and document this in their business risk assessment.

Where a firm decides to apply a different standard of CDD measure in circumstances where it believes, following a risk assessment, that a lower level of ML/TF risk applies, the firm should document its rationale for this. This would assist the firm in demonstrating to the Central Bank that it has complied with its obligations under the CJA2010 and CJA2018 (as amended).

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 may qualify them as a low risk level.

Protection/Pension	Typical Features
1 Term life assurance	▪ Only pays out on death of policy holder ▪ No surrender value ▪ Small, regular premiums: additional payments by customer not possible ▪ Large premiums will normally require medical evidence ▪ 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 ▪ No surrender value ▪ 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 ▪ No surrender value ▪ Small, regular premiums: additional payments by customer are not possible
4 Whole of Life	▪ May accrue some small surrender value ▪ Benefits usually payable on death or diagnosis of terminal illness or in some cases, critical illness of the policyholder ▪ Partial surrenders are normally allowed within specified limits
5 Pensions	▪ Revenue approved pensions

- Generally, for protection products with annual premium of more than €1000, due diligence requirements are satisfied by the Name, Address and Date of Birth 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 policy owner's own 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 and request completion of the source of funds form Appendix 7.

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 With premium under €5000 Investment Bonds with premium under €5000	▪ Long term savings plan often for retirement ▪ Requires at least five years to gain positive return on investment ▪ Often unable to be surrendered in first or second year, with penalties in years three to five ▪ Additional 'top up' payments may be permitted
Endowments	▪ Long term savings plan for a set term(were often linked to mortgages) ▪ Usually long term, 10-25 years
ARFs & AMRF	▪ Post retirement pension products

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:

- Name, address and date of birth collected on the application form in conjuction with the fact that the payment is made from an account in the policy owner's name (ie. personal cheques and other payment instruments drawn on policy owner's account such as Direct Debits/Standing Orders)

- If payment is not by way of Direct Debit/personal cheque drawn on policy owners own account, complete source of funds form (Appendix 7)

- Certified copies of identification and proof of address for policy owner and third party if applicable.

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: ▪ With profits ▪ Guaranteed ▪ Income ▪ Investment ▪ Offshore international bonds	▪ Open ended investment ▪ Usually a 5 year recommended ▪ minimum investment term but can be surrendered earlier ▪ Additional 'top up' payments permitted by the policy holder and by third parties ▪ May be segmented and individual segments may be assignable

Due Diligence Requirements:

- Name, address and date of birth collected on the application form in conjunction with the fact that the payment is made from an account in the policy owner's name (i.e. personal cheques and other payment instruments drawn on policy owner's account such as Direct Debits/Standing Orders)
- Certified copies of identification and proof of address for policy owner and third party if applicable.
- Complete source of Wealth form (Appendix 8).

How to Identify?

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;

The Central Bank has not provided prescriptive/definitive examples of documentation that it considers would satisfy customer identification and verification requirements. However, they have stated that firms should maintain their own lists of documents which they will accept for the purposes of identification/verification. These lists should be subject to review to ensure that they remain current and appropriate, taking into account their evolving processes, and adoption of new technology.

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 8

Additional requirements for PEPs

Firms' policies and procedures must address how any PEP relationships identified will be managed by the firm including:

- Application of EDD measures to PEPs, including determining Source of Wealth and Source of Funds (Appendix 8);
- Obtaining Senior Management Approval or equivalent - Firms should put appropriate policies and procedures in place clearly setting out;
  - The reporting and escalation of PEP relationships to Senior Management or equivalent;
  - The timelines for obtaining Senior Management or equivalent sign-off; and
  - The level of seniority required in order to approve a PEP relationship; and
- Enhanced on-going monitoring measures.

Ongoing Monitoring

Designated persons should undertake monitoring/periodic client reviews on an ongoing basis for patterns of unusual or suspicious activity to ensure that higher risk activity is scrutinised.

When assessing CDD obligations in relation to the on-going monitoring of customers, firms should ensure that they have effective and appropriate on-going monitoring policies and procedures that are in place, in operation and adhered to by all staff. Such policies and procedures should include at a minimum:

- Full review and consideration of all trigger events associated with their customers. Clear examples of trigger events that are understood by staff and targeted training should be provided for staff on how to identify possible trigger events and interpret these. Trigger events should also be reviewed on a regular basis by the firm and examples revised where appropriate;

- A well-documented and well-established monitoring programme, which is demonstrative of a risk-based approach, where high-risk customers are reviewed on a frequent basis;

- Periodic reviews of customers, the frequency of which is commensurate with the level of ML/TF risk posed by the customer. Firms should also ensure that staff are provided with specific training on how to undertake a periodic review;

- Reassessment and, if applicable, re-categorisation of customers upon material updates to CDD information and/or other records gathered through a trigger event or periodic review;

- Re-categorisation of customers as high risk subject to Senior Management or equivalent approval and the completion of enhanced due diligence before a decision is taken to continue the relationship;

- Screening undertaken of all customers to identify new and on-going PEP relationships. The frequency of such screening should to be determined by the firm, commensurate with the firm's business risk assessment;

- Clear instruction for staff regarding the action required where appropriate CDD documentation or information is not held on file. Such instruction should include the steps that may be taken to locate or obtain such documentation or information; and

- Proactive utilisation of customer contact as an opportunity to update CDD information.

"Complex or unusually large" transactions, or "unusual patterns of transactions" must be investigated in greater detail and monitoring increased if they appear suspicious. Firms should attempt to establish the rationale for changes in behaviour and take appropriate measures, for example, by conducting additional due diligence.

Firms should put in place adequate policies and procedures to identify unusual transactions or patterns of transactions. Examples may include transactions or patterns of transactions that are:

- Larger than the Firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
- Of an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- Very complex compared with other similar transactions associated with similar customer types, products, or services; and the Firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

Where Firms detect unusual transactions or patterns of transactions, they should apply EDD measures sufficient to help the Firm determine whether these transactions give rise to suspicion.

Such EDD measures should at least include:

- Taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- Monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A Firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

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 ML/TF is to examine the intended use or destination of the funds as opposed to its origin.

Transaction monitoring

For transaction monitoring controls to be effective, they must detect what suspicious activity looks like in the context of the designated person's business activities and in the context of the designated person's specific customer profile(s). As such, the controls should be tailored to the designated person's business risk assessment, and the customer risk assessment. By using the business wide risk assessment, a designated person can determine the appropriate transaction monitoring solution for that designated person's specific business activities. There should be a mechanism for making changes to controls to take into account altering risk and new risk indicators, for example COVID 19.

The Central Bank expects to see connectivity between a designated person's CDD, transaction monitoring, and STR processes. A designated person should have sufficient and up to date information on file and obtained during the CDD process to determine whether transactional activity is suspicious.

Management Responsibilities

The Senior Management, including the Board of Directors (the 'Board'), have responsibility for managing the identified ML/TF risks by demonstrating active engagement in the firms' approach to effectively mitigating such risks. Firms should ensure that the AML/CFT role and responsibilities of Senior Management is clearly defined and documented.

The Principal/Sole trader should take responsibility for managing the risks and must demonstrate and record the consideration of ML/TF risks and their approach to mitigate the risks. The Principal/Sole trader must perform and evidence the tasks as listed below.

Firms should ensure that there is appropriate governance and oversight with regard to its compliance with obligations under the CJA 2010. For example, firms should ensure for:

Business risk assessments:

- Senior Management, or equivalent, has reviewed and approved the methodology used for undertaking the Firm's business risk assessment.
- Senior Management, or equivalent, has reviewed and approved the firm's business risk assessment at least on an annual basis to ensure that it is aware of the ML/TF risks facing the firm and that the corresponding AML/CFT measures which the firm has in place are appropriate for the level of ML/TF risk identified.

Policies and Procedures

- Senior Management, or equivalent, has reviewed and approved all policies and procedures, and material updates to same.

Reporting Lines:

- Appropriate reporting lines are in place to facilitate the escalation of AML/CFT issues from the MLRO for discussion at Senior Management or equivalent level.

Senior Management/Sole Trader/One director company meeting:

- AML/CFT issues appear as an agenda item at regular intervals at Senior Management meeting(s) and that the corresponding minutes reflect the level of discussion and outcomes, which take place concerning any Management Information (MI) provided by the MLRO or any particular AML/CFT/FS issues requiring discussion by the Senior Management. In the case of Sole Traders, or one director companies, the evidence of consideration given to these issues, and the decisions made should be documented.
- The MLRO delivers a report to Senior Management, or equivalent, at least on an annual basis and that a detailed discussion on its content takes place with a corresponding minute to reflect the level of discussion.
- The MI provided to Senior Management, or equivalent, to include information on training, training completion and training pass rates.

On-going monitoring

- Senior Management, or equivalent, should approve the re-categorisation of customers as high risk before a decision is taken to continue the business relationship

High Risk Third Country

- Senior Management, or equivalent, approval must be obtained to commence or continue the business relationship with a customer, to ensure that Senior Management or equivalent are aware of the risk their firm is exposed to and can make an informed decision about the extent to which the firm is equipped to manage that risk;

AML/CFT Resourcing

- The firm's AML/CFT function is adequately resourced (both in terms of staff and systems) commensurate with the level of ML/TF risk faced by the firm.
- Reviews are undertaken on a regular and timely basis to consider whether the firm has the appropriate staff numbers, the correct skill-set and whether staff have access to adequate systems and other resources to effectively perform their role as it relates to AML/CFT issues.

Firms should ensure that appropriate evidence of discussions at Senior Management meetings and/or approvals concerning AML/CFT issues are recorded and retained in accordance with the firm's record retention policy. In the case of Sole Traders, or one director companies, the evidence of consideration given to these issues, and the decisions made should be recorded and retained in accordance with the firm's record retention policy.

Firms should also ensure that appropriate evidence is retained in accordance with its record retention policy regarding the firm's obligations in relation to:

Politically Exposed Persons (PEPs):
Retention of Senior Management, or equivalent, approvals of all new PEP relationships which a firm enters into or where the PEP status of a customer subsequently changes during the course of a relationship with a firm as required under Section 37 of the CJA 2010.

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. A copy of these board meeting minutes should be kept on file. For Soletraders, record should be kept of issues and decisions made.

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 and it should be recorded that procedures have being updated to reflect the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018. See Appendix 9

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 firm's 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 policies and procedures must be supplemented by guidance, accurately reflect the firm's operational practices and demonstrate consideration of and compliance with all legal and regulatory requirements and are to be made available to all staff. 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) the documents and information which the firm is willing to accept and the circumstances under which they are willing to accept them in order to identify and verify the identity of a customer,
(c) customer due diligence measures – specify the timeframe for which CDD must be completed,
(d) the identification of the most appropriate simplified due diligence measures the firm will apply to business relationships or transactions,
(e) monitoring transactions and business relationships,
(f) 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,

(g) the firm's approach with regard to the identification, assessment, selection and monitoring of third-party relationships, including the frequency of testing performed on such Third Parties,
(h) the firm's approach to identifying if a customer/beneficial owner is a PEP, and if a customer becomes a PEP during the course of the business relationship and how the firm will manage these relationships,
(i) the reporting and escalation of PEP relationships to Senior Management or equivalent, the timelines for obtaining Senior Management or equivalent sign-off, and the level of seniority required in order to approve a PEP relationship,
(j) how the firm reviews its customer base against Financial Sanctions lists,
(k) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,
(l) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments,
(m) reporting (including the reporting of suspicious transactions),
(n) record keeping,
(o) measures to be taken to keep documents and information relating to the customers person up to date,
(p) measures to be taken to keep documents and information relating to risk assessments up to date,
(q) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and
(r) 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, or equivalent, 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. Firms should keep adequate records, including:

- All documentation and information obtained for the purposes of identifying and verifying a customer, person(s) authorised to act on behalf of the customer and any beneficial owners;
- All customer risk assessments;
- Copies of all additional documentation and information obtained, where EDD measures have been applied to a customer of the firm;
- Evidence of any sample testing of CDD files, which the firm has undertaken as part of its assurance testing process; and
- Copies of documentation and information obtained as part of the firm's ongoing monitoring process.
- Copies of all transactions carried out for the customer

- verification and evidence of the on-going monitoring conducted by the firm, including the monitoring of transactions, the results of such monitoring and decisions taken on foot of on-going monitoring
- Reporting of suspicious transactions
- Training provided to staff, directors and other office holders
- Firms should retain all records of discussions and decisions made at Senior Management or equivalent level in relation to:
    - How the requirements of the CJA 2010 were assessed and implemented; and
    - Any AML/CFT issues as they arise on an on-going basis.

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.

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.

Firms should consider the outcomes of their own Business Wide Risk Assessments and whether the frequency and content of AML/CFT training provided is adequate for levels of ML/TF risks faced by the firm.

It is recommended that annual anti-money laundering training be provided to staff on an annual basis. Firms should ensure that AML/CFT training is provided to all new recruits upon joining the firm in a timely manner and to all staff at least on an annual basis thereafter. 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.

Firms should also provide enhanced AML/CFT training tailored to the specific needs of staff who perform key AML/CFT and FS roles within the firm, for example the firm's MLRO or Senior Management or equivalent responsible for AML/CFT oversight.

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. This includes non-exec directors.

Firms should ensure that the AML/CFT training provided includes an assessment or examination during the training session, which should be passed by all participants in order for the AML/CFT training to be recorded as completed. If the training does not contain an assessment or examination, firms must be in a position to demonstrate effectiveness of training and staff understanding in relation to same.

Firms should keep a comprehensive record of:

- all staff, Senior Management and agents who have received AML/CFT training;
- the dates on which AML/CFT training was provided;
- the nature and content of AML/CFT training provided;
- the date on which the AML/CFT training was provided; and
- Results of the assessment and examination during the training session.

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.

Firms should consider their specific products, services and customers when making a determination of suspicion, as what might be considered suspicious for one product, service or customer may not be for another. The following is a non-exhaustive list of examples of what might raise suspicions:

- Transactions or a series of transactions that appear to be unnecessarily complex, making it difficult to identify the beneficial owner or that do not appear to make economic sense;
- Transaction activities (in terms of both amount and volume) that do not appear to be in line with the expected level of activity for the customer and/or are inconsistent with the customer's previous activity;
- Transactions in excess of a customer's stated income;
- Large unexplained cash lodgements;
- Loan repayments inconsistent with a customer's stated income, or early repayment of a loan followed by an application for another loan;
- Requests for third party payments. For example, this might include a third party making a payment into a customer's account to pay off a loan, to fund an investment or policy, or to fund a savings account;
- Refusal to provide customer due diligence documentation or providing what appears to be forged documentation.

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 (STRs) - Section 42(2) of the CJA 2010 requires firms to make an STR "as soon as practicable …"

'As soon as practicable' means when the firm acquires that knowledge, forms a suspicion, or acquires those reasonable grounds to suspect money laundering or terrorist financing. The firm may need to conduct further analysis and assessment in order to make its determination. Any such analysis and assessment should be conducted without delay, however as soon as the firm has established knowledge, a suspicion or reasonable grounds to suspect, it should immediately file an STR.

All reports submitted via the internal reporting process should be recorded. The internal reporting procedure should at least document:

- All required steps for the reporting of suspicions from staff to the MLRO, or any other person(s) charged under the firm's internal reporting process with investigating suspicions, and from the MLRO to the authorities;
- The timeframes for escalation of suspicious transactions from when a staff member first identifies a suspicious transaction to when it is raised;
- Formal acknowledgement by the firm's MLRO or any other person(s) charged under the firm's internal reporting process with investigating suspicions raised internally by staff; and
- Information with regard to 'Tipping-off' so as to ensure that staff are aware of their obligations under the CJA 2010, the penalties for the offence of Tipping Off and that they exercise caution after the filing of an STR.

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 FIU 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.

STRs submitted to FIU Ireland should be made via the goAML application. Firms should ensure that they are registered with goAML as STRs cannot be submitted via goAML unless the firm has previously registered.

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.

STRs must be submitted to Revenue using the Revenue's Online Service (ROS) only. To submit an STR online, the designated person must firstly be registered for ROS and have a digital certificate. You can then register for STR Reporting and request a sub user certificate for all MLROs. For further guidance on submitting STRs online, please see the Revenue Website.

Section 54 of the CJA 2010 requires a designated person to adopt policies and procedures to prevent and detect the commission of ML/TF. The Central Bank expects that all designated persons are registered with ROS.

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 FIU/Revenue Commissioners in relation to suspicions of money laundering or terrorist financing.

Firms should keep sufficient records in relation to suspicious transactions, including:

- The circumstances that gave rise to the suspicion;
- Any additional monitoring/assessment that was undertaken;
- Whether the suspicion was reported/not reported, and
- Rationale for reporting or not reporting to FIU Ireland and the Revenue Commissioners.

Firms should retain copies of all documentation and information used as part of any internal assessment into a customer following on from the filing of an internal STR by a staff member. Firms should also retain records to provide evidence and the justification behind their decision whether or not to file an STR with FIU Ireland and the Revenue Commissioners. In this regard, firms should also retain copies of the supporting documentation and information which assisted them in reaching their decision.

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:

UN Sanctions Committees:
https://www.un.org/sc/suborg/en/sanctions/information
https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

EU sanctions:
https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-listsanctions_en
https://eeas.europa.eu/headquarters/headquarters-homepage/423/sanctions-policy_en

Many Broker CRM systems have the facility to conduct this sanction checking – members are advised to contact their CRM provider to see if this service is included and to determine how records are kept that this check is been carried out.

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

In the event that a match or a 'hit' occurs against a sanctioned individual or entity, the firm must immediately freeze the account and/or stop the transaction and immediately report the hit to the Central Bank along with other relevant information by using the following email sanctions@centralbank.ie

Before submitting a report to the Central Bank, the institution should take reasonable steps to ensure that the person or entity identified is the same person or entity as that listed in the relevant sanctions list (i.e. verifying the name, date of birth address with other identifying information).

Roles & Responsibilities of the Money Laundering Reporting Officer

Firms should ensure that the person appointed as MLRO:

- Has sufficient and appropriate AML/CFT knowledge and expertise;
- Has the autonomy, authority and influence within the firm to allow them to discharge their duties effectively;
- Is capable of providing effective challenge within the firm on AML/CFT matters when necessary;
- Has the capabilities, capacity and experience to oversee the identification and assessment of suspicious transactions and to report/liaise with the relevant authorities where necessary in relation to such transactions;
- Keeps up to date with current and emerging ML/TF trends and issues in the industry and understands how such issues may impact the firm;
- Has access to adequate resources and information to allow them to discharge their duties effectively; and
- Is readily accessible to staff on AML/CFT matters.

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 transaction's 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 which is proportionate to the nature, scale and complexities of the firm's activities, provide comment on the

effectiveness of the firms AML/CFT systems and controls, and include recommendations for improvement.

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.

Appendix 1

EXPECTATIONS OF THE CENTRAL BANK ON NON-LIFE INTERMEDIARIES

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 knowledge or suspicions of money laundering transactions. Staff would need to be trained also in this regard.

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.

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).

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.

A timeframe should be set on when the next risk assessment will take place.

Executive Summary

- Confirm Brokerage's name, address and legal status
- Detail current Authorised status: IIA, IDR, 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
- Has there been an increase in trigger events resulting in internal suspicious transaction reports or compliance failures which have a bearing on the firm's risk assessment?

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:

---

[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.

Does the firm capture and review information on risks relating to new products?

_____
_____

Risk Assessment Sheet

Product Name	Product AML CTF risk rating	No. of Customers	No. of Customers rated High Risk (excluding PEPS)	No. of Customer rated Medium Risk	No. of Customers rated Low Risk	No. of PEPs
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

Firms must identify and assess the ML/TF risk in relation to a customer. The risks to be considered would include the customer's and their beneficial owner's business or professional activity, their reputation and their nature and behaviour.

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 check all clients against the EU/UN sanctions listing?

_____

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: _____
Reviewed by the Board _____
Next Risk Assessment Review Date: _____

Appendix 3

Risk Based Assessment on Customers

In order to comply with the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010 and, the 4th EU Anti Money Laundering Directive

Firms must identify and assess the ML/TF risk in relation to a customer. The risks to be considered would include the customer's and their beneficial owner's business or professional activity, their reputation and their nature and behaviour.

- Did the firm meet the Customer Face-to-Face? Yes _____ No _____

If yes, the name of the individual who met the applicant Face-to-Face:
Staff member: _____
If No, has additional Due Diligence measures been undertaken _____

- Customer's Country of Birth: _____
- Customer's Country of Residence: _____
- Customer's Occupation: _____

- Did your firm check the clients against the EU/UN sanctions listing? Y/N
  If no explain the rationale:
  _____

- Customer's overall Source of Wealth
  - Savings from Regular Income
  - Windfall / Winnings
  - Bonus
  - Interest or Dividends
  - Retirement / Redundancy
  - Sale of Asset
  - Inheritance / Gift
  - Court Awarded Settlement
  - Other

    _____
    _____
    _____

- Source of Funds being used to pay premium/repay the loan

  - Salary / Social Welfare Payment
  - Pension
  - Rental Income
  - Savings / Investments
  - Other

    _____
    _____
    _____

Completed by: _____
Dated: _____

Appendix 4

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.".

Appendix 6

Brokers Ireland would recommend that members use a PEP search platform to check for PEPs: however, in the absence of this, this should be completed with the client at a minimum.

[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: / /

Appendix 7
Source of Funds

Payment made by:

Personal cheque/Direct Debit from Policy Owners own Bank account ☐

Or

Third Party cheque/Direct Debit ☐

Payor Name (If Third Party) & Nature of relationship between Third Party Payor to Policy Owner:

_____

Or

For Bank Drafts, provide details of the bank account from which the funds will be paid:

Name of Bank/Building Society: _____

IBAN: _____

BIC: _____

Country account is based in: _____

Payor Name (If Third Party) & Nature of relationship between Third Party Payor to Policy Owner:

_____

Or

Maturity of existing Policy

Policy Details: _____

Name of Provider: _____

Or

Other:

Give Details: _____

Appendix 8
Source of Wealth

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	

Appendix 9

DECLARATION OF COMPLIANCE WITH THE MONEY LAUNDERING PROVISIONS OF THE MONEY LAUNDERING PROVISIONS OF the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010 and the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

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

The Irish AML/CTF legislative framework is set out in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. This framework was updated with the transposition of the 4th EU AML Directive into Irish Law in 2018 pursuant to the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

I/We confirm that the firm's policies and procedures have been updated to reflect the changes contained in the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 with regards to the following:

- Introduction of business risk assessments
- Changes to Customer due diligence requirements
- Monitoring
- Politically Exposed Persons
- Beneficial Ownership
- Record Keeping

Additional comments

_____
_____
_____
_____
_____
_____

Signed by: _____ Date:_____

Full Name: _____

Role Held: _____

Reviewed by the Board: _____ Date:_____