Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

2016

Report on Anti-Money Laundering/Countering the Financing of Terrorism and Financial Sanctions Compliance in the Life Insurance Sector in Ireland

Contents

1. OVERVIEW

1.1 INTRODUCTION

This Report (the "Report") sets out the observations and expectations of the Central Bank of Ireland (the "Central Bank") in relation to Anti-Money Laundering ("AML")/Countering the Financing of Terrorism ("CFT") and Financial Sanctions ("FS") compliance by life insurance firms in Ireland ("firms")

The Report is based on a combination of on-site inspections and off-site desk top reviews carried out by the Central Bank over the course of 2014 and 2015. The Report is not legal advice and should not be treated as such. A firm must at all times refer directly to the relevant legislation to ascertain its statutory obligations.

1.2 BACKGROUND

The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended by the Criminal Justice Act 2013) (the "CJA 2010") specified the Central Bank as the State's competent authority for the effective monitoring of credit and financial institutions ("designated persons") for compliance with the CJA 2010. Section 63 of the CJA 2010 requires the Central Bank to effectively monitor designated persons and take measures that are reasonably necessary for the purpose of securing compliance by those designated persons with the requirements specified in Part 4 of the CJA 2010. Under Section 25(6) of the CJA 2010, a designated person also includes an insurance firm operating in Ireland by means of a branch.

Compliance with the CJA 2010 is a legally enforceable obligation, breaches of which are subject to criminal and/or administrative sanctions. Effective AML/CFT and FS compliance will only occur where firms understand the risks applicable to their own business and implement controls that are appropriate to effectively mitigate those risks.

1.3 METHODOLOGY

The Report was compiled using a combination of both on-site and off-site elements which are outlined in more detail below.

ON-SITE

AML/CFT and FS on-site inspections were carried out focusing on the following areas:

- AML/CFT and FS compliance governance structures and controls, including:
  - Governance structures;
  - Risk Assessment;
  - Policies, processes and procedures;
  - Outsourcing;
  - Training;
  - Management Information;
  - Internal Controls.
- Customer Due Diligence ("CDD"), including:
  - On-boarding of new policyholders;
  - On-going monitoring;
  - Reliance on third parties.
- Suspicious Transaction Reporting, including:
  - Transaction monitoring;
  - Process for identification and escalation of suspicious transactions.
- Testing of AML/CFT and FS IT systems.
- EU Financial Sanctions.

The inspections, which were carried out over the course of 2014 and 2015, comprised of:

- A review of relevant policies, procedures, risk assessments, Management Information ("MI") as well as internal audit and compliance reports;
- Interviews with key senior staff, including the Money Laundering Reporting Officer ("MLRO");
- A review of any Third Party Reliance arrangements in place;
- A review of outsourcing arrangements in place;
- On-site walk-throughs of key AML/CFT and FS processes;
- A review of IT systems used by firms as part of their AML/CFT and FS framework including, but not limited to, systems used for the purposes of screening policyholders against Politically Exposed Persons ("PEPs") and EU Financial Sanctions lists, monitoring

systems and system access controls;

- Sample testing of CDD documentation and/or information, Suspicious Transaction Report (STR) records, Third Party Reliance & outsourcing arrangements and records of transaction monitoring and assurance testing conducted.

OFF-SITE

The on-site inspections were supplemented by off-site desk top reviews. Desk top reviews facilitate an analysis by the Central Bank of Money Laundering/Terrorist Financing ("ML/TF") risk through an evaluation of key pieces of documentary evidence such as the firm's Risk Assessment and Policy and Procedures.

1.4 SUMMARY OF ISSUES IDENTIFIED

While all of the issues did not arise in any one firm, they are representative of issues identified across all the firms included as part of the review. The issues identified, which are set out in more detail in the remainder of the Report, include:

- Non-adherence to stated AML/CFT and FS policies;
- Weaknesses in the suspicious transaction reporting process. In particular a lack of documentary evidence of the assessment and adjudication performed by the MLRO on the rationale for reporting or not reporting to the relevant authorities;
- Deficiencies in the on-going customer and transaction monitoring processes;
- Insufficient evidence of firms giving sufficient consideration to the requirements of Section 33(1)(d) of the CJA 2010 in order to determine the adequacy of documentation and/or information held for existing policyholders on-boarded pre-July 2010. Where trigger events were in place to collect or update CDD, these were deemed insufficient;
- Deficiencies in the policies and processes in place relating to third party reliance and outsourcing arrangements;
- Deficiencies in the policies and procedures in place with respect to the definition and identification of PEPs and application of Enhanced Due Diligence ("EDD") including the obtaining and timing of senior management approval and the failure to sufficiently identify, verify and document Source of Funds ("SOF") and Source of Wealth ("SOW");
- Failure by firms to fully consider, qualify or document the criteria and process for the identification, recording, and application of EDD to high risk policyholders.

1.5 CONCLUSION

The Central Bank acknowledges that in many instances, firms had satisfactory procedures and systems and controls in place. However, the issues identified highlight that further enhancements could be made by firms to strengthen their existing AML/CFT and FS frameworks. The life insurance sector in Ireland offers a diverse range of products sold through a range of distribution channels, both domestically and cross border. Although the inherent risk of Money Laundering and Terrorist Financing may be lower than in other sectors, firms need to be cognisant that there are products, customers and geographic regions that present a higher risk of Money Laundering and Terrorist Financing. While the life insurance sector in Ireland is the specific focus of the Report, many of the issues raised are relevant to the broader financial services sector in Ireland. The Central Bank expects all financial and credit institutions to carefully consider the issues raised in the Report, and to use the Report to inform the development of AML/CFT and FS frameworks.

2. GOVERNANCE & COMPLIANCE

In accordance with Section 54(1) of the CJA 2010, all firms must adopt policies and procedures to prevent and detect the commission of ML/TF. Insufficient or absent AML/CFT risk management policies, procedures and processes exposes firms to significant risks, including not only financial but also reputational, operational and compliance risks. The adopted risk management measures should be risk-based and proportionate, informed by a firm's individual assessment of its Money Laundering/Terrorist Financing risk exposure and in compliance with the legislation. The Board of Directors (the "Board") and senior management must take responsibility for managing the identified risks by demonstrating active engagement in a firm's approach to effectively mitigating such risks.

2.1 BUSINESS-WIDE ASSESSMENT OF MONEY LAUNDERING/TERRORIST FINANCING RISK

The assessment of ML/TF risk exposure is essential to the effective development of policies and procedures and to a firm's ability to apply proportionate systems and controls. The life insurance sector provides a diverse range of products through a number of distribution channels.

In assessing the approach taken by firms to conducting ML/TF risk assessments, the Central Bank noted that the majority of firms inspected had undertaken and documented a ML/TF risk assessment of their business. Most assessments reviewed had given some consideration to risk categories (such as geographic risk, product/service risk, policyholder risk and channel/distribution risk). However, product risk was highlighted as the primary driver, reflecting the view of the industry that the majority of the products offered do not deliver sufficient functionality and flexibility to be the first choice of vehicle for money laundering or terrorist financing. While the features of certain products may help to reduce the ML/TF risk, it is important that firms do not place over reliance on this element of the assessment and that appropriate weight is also given to the other risk factors.

The Central Bank identified a number of inadequate practices, such as:

- Insufficient evidence that firms had completed an adequate ML/TF risk assessment of their legacy business, including books of business taken on through acquisition or merger;
- Insufficient documented rationale underpinning the basis for the conclusions outlined in the risk assessment e.g. lacking in specifics on policyholder risk, PEPs, statistical analysis etc.;

- Insufficient documentary evidence of meetings held and decisions taken when drafting or reviewing the risk assessment for the firm.

In carrying out risk assessments, the Central Bank expects that:

- Firms undertake and document a ML/TF risk assessment of their business, to include all risk categories (such as geographic risk, product/service risk, policyholder risk and channel/distribution risk);
- The underlying methodology, assumptions and risk ratings used are documented to ensure that there is an objective validation of the risk assessment;
- Identified risks are assigned a risk rating having regard to the systems and controls in place to manage those risks;
- Appropriate controls are devised to mitigate any risks identified and that these controls are aligned to and embedded in operational procedures;
- The risk assessment identifies any gaps, with action plans recorded to address such gaps;
- Risk assessments are reviewed and approved by the Board at least annually and are used to inform the firm's approach to the management of ML/TF risk;
- Risk assessments are also reviewed and updated in line with business developments and changes in risk categories (such as geographic risk, product/service risk, policyholder risk and channel/distribution risk).

2.2 ROLES & RESPONSIBILITIES

The Board is ultimately responsible for ensuring compliance with the CJA 2010. Firms must put in place appropriate AML/CFT structures that reflect the nature, scale and complexities of their activities. The Central Bank noted that many of the firms inspected did not have a dedicated AML/CFT function, but rather AML/CFT responsibilities were assigned to another function, such as the Compliance Function. In such circumstances, the Board must ensure that AML/CFT issues receive sufficient attention amidst broader compliance activities undertaken. When assessing the governance structures in place, the Central Bank noted a number of inadequate practices, including:

- The roles and responsibilities of the Board and senior management with regard to AML/CFT were not clearly defined or documented in the firms' policies;
- There was a lack of detail as to how Board and senior management were kept informed of AML/CFT matters on an on-going basis;
- There was a lack of oversight exercised by firms' senior management over key elements of the AML/CFT framework where these elements were outsourced.

In assessing the Governance structures in place the Central Bank expects that:

- There is a clearly established organisational structure that reflects the responsibility for AML/CFT management based upon the nature, size and complexity of the firm;
- The roles and responsibilities of the Board, senior management and the MLRO regarding AML/CFT are clearly defined and documented;
- The Board and senior management can demonstrate active engagement in the monitoring and management of ML/TF risk, including:
  - Involvement in completion of the ML/TF risk assessment;
  - Effective flows of good quality MI, resulting proactive mitigating actions and timely closure and resolution of issues;
  - Regular assessment and evaluation of regulatory changes as well as consideration of industry developments that may impact the business;
- The MLRO is independent, knowledgeable and provides effective challenge to the business when necessary;
- The function assigned responsibility for AML/CFT is adequately resourced for this purpose e.g. Compliance Function.

2.3 POLICIES & PROCEDURES

In accordance with Section 54(1) of the CJA 2010, firms must adopt policies and procedures to prevent and detect the commission of Money Laundering/Terrorist Financing.

In assessing the policies and procedures in place, the Central Bank found a number of inadequate practices, including:

- Lack of evidence that policies and procedures in place were reviewed on a regular basis and revised in a timely manner;
- Policies and procedures did not adequately reflect actual operational practices;
- Documented policies and procedures were not being fully adhered to in all cases e.g. triggers to update CDD were not being observed;
- Policies and procedures in place did not demonstrate that the firms had adequately considered or fully provided for all of their obligations under the CJA 2010 such as:
  - Ensuring that prior to claim pay out, all beneficiaries are subject to screening against PEP and FS lists;
  - The criteria by which the firm would define and identify both new and existing policyholders as High Risk for the purpose of applying the appropriate level of due diligence as prescribed under Sections 37 and 39;
  - Ensuring sufficient and risk based transaction and on-going monitoring of

policyholders as prescribed under Section 35(3).

When developing AML/CFT policies and procedures, the Central Bank expects that firms:

- Maintain a detailed suite of AML/CFT policies, which are supplemented by guidance and supporting procedures that fully demonstrate consideration of and compliance with all legal and regulatory requirements;
- Have a clearly defined process in place for the formal review and approval, at least annually, of the policies and procedures at appropriate levels;
- Policies and procedures are reviewed and updated in response to events or emerging risks;
- Policies and procedures are readily available to all staff and are fully implemented and adhered to;
- Policies and procedures are subject to independent review and testing.

2.4 OUTSOURCING

Firms may use third party service providers (including other group entities) to perform various elements of their AML/CFT activities on a contractual basis, often in outsourcing/agent relationships. However, the firm remains responsible for compliance with its obligations under the CJA 2010.

In assessing the firms' outsourcing arrangements, the Central Bank noted that:

- In some instances, where group outsourcing arrangements were used, written contracts/Service Level Agreements ("SLAs") were not in place for all AML/CFT activities that were outsourced;
- The level of Board oversight in respect of such arrangements was insufficient.

When outsourcing some or all AML/CFT activities to a third party service provider (either an external party or other group entity), the Central Bank expects firms:

- To have robust policies and procedures in place in relation to outsourcing arrangements together with written contracts and SLAs clearly setting out the obligations and responsibilities of the respective parties;
- To ensure that all such arrangements are subject to sufficient oversight, review and testing to ascertain if they are operating as intended;

- To ensure AML/CFT procedures applied reflect those of the firm, notwithstanding whether the outsourced service provider is a related group entity or comes from outside the group.

2.5 TRAINING

Section 54(6) of the CJA 2010 requires firms to ensure that staff are aware of the law relating to Money Laundering/Terrorist Financing and are provided with on-going training. In assessing the nature, extent and frequency of the training provided, the Central Bank found a number of inadequate practices in place, including:

- Insufficient evidence that staff in key roles relating to AML/CFT had received appropriate training;
- AML/CFT policy did not specify or contain sufficient detail on how AML/CFT training will be provided, the format of delivery, and how completion of training will be tracked and monitored.

In relation to firms' training obligations, the Central Bank expects that:

- Firms have a documented and on-going training plan in place to ensure appropriate levels of AML/CFT training are provided to the Board and all staff involved in the conduct of the business (including staff at outsourced service providers);
- Training content is reviewed and updated on a regular basis to ensure it remains current and appropriate and the material is signed off by senior management;
- Enhanced training is provided to senior management and staff in key AML/CFT roles to ensure their knowledge remains adequate and up-to-date;
- Training records are maintained and relevant MI is circulated to senior management.

2.6 RECORD KEEPING

Section 55 of the CJA 2010 requires firms to keep records evidencing procedures applied and information obtained to verify the identity of customers and beneficial owners. In addition it specifies that firms shall keep records evidencing the history of services and transactions carried out in relation to their customers.[1]

The Central Bank observed the following inadequacies in relation to record retention in firms:

- A number of CDD files reviewed were of poor quality and it was difficult to ascertain if sufficient verification of policyholders' information was obtained;
- The AML/CFT policy and procedures did not contain any detail on the record keeping requirements of the CJA 2010.

In assessing the firms' approach to record keeping, the Central Bank expects that:

- Firms have a documented record retention policy and procedures relating to all records relevant to their AML/CFT framework;
- Assurance testing is conducted at appropriate intervals to ensure the quality and legibility of documents held and that records are being retained and/or destroyed in line with the firms' policy and the relevant legislative provisions.

[1] In this regard, firms should also consider the requirements set out in provision 11.6 of the Consumer Protection Code 2012.

3. CUSTOMER DUE DILIGENCE

In accordance with Section 33(2) or (4) of the CJA 2010, firms are required to identify and verify ("ID&V") customers and, where applicable, the beneficial owner(s), prior to the establishment of a business relationship or the carrying out of a transaction or service.

Sections 33(5), (6) and (7), 34 and 36 of the CJA 2010, offer certain exceptions to the general rules established in Section 33(2) or (4) of the CJA 2010, some of which are specific to the life insurance industry.

Section 33(7) of the CJA 2010 permits the verification of the identity of such a beneficiary to be completed after the business relationship has been established but prior to the policy being paid out or the beneficiary exercising any other vested rights under the policy. In addition Sections 34 and 36 of the CJA 2010 exempt firms from applying measures specified in Sections 33(2) and 35(1) of the CJA 2010 where the firm can demonstrate that the product or customer is a specified product or customer as defined under Section 34(5) and (7) of the CJA 2010. The Central Bank found that these exceptions were widely applied across the sector, with CDD for many policyholders either deferred to claim stage or Simplified Customer Due Diligence ("SCDD") applied due to the specified product categorisation.

In all cases where the exceptional approach to the general rules established in Section 33(2) and 35(1) of the CJA 2010 is taken, firms must be mindful that the exceptions do not apply in circumstances where:

- The customer concerned is from a place that is designated under section 32;
- Section 33(1)(c) or (d) or (4) applies; or
- Measures under Section 37 in respect of PEPs apply.

One of the features of the life insurance sector is that products are often sold through intermediaries i.e. brokers[2], in which case the intermediary in question is best placed to conduct the required due diligence on prospective policyholders. In these scenarios, firms may choose to obtain the due diligence documentation and/or information from the intermediary and retain the records themselves or they may choose to rely on the intermediary to obtain and retain the documentation and/or information. In the latter situation, where reliance of this sort is placed on an intermediary, firms must ensure that such an arrangement is in line with Section 40 of the CJA 2010. Further information on the

[2] For the avoidance of doubt, under the CJA 2010 tied agents are not separate designated persons from the life company that has appointed them as their agent.

establishment and monitoring of 'third party reliance arrangements' is outlined in section 3.4 of this report.

3.1 ON-BOARDING NEW POLICYHOLDERS

The Central Bank identified the following inadequate practices in relation to new policyholders:

- Firms not obtaining sufficient information and documentation, in some instances, to fully identify the policyholder and/or beneficial owner(s) in order to satisfy the required amount of due diligence applicable;
- Policies and procedures do not clearly define or document the requirements for determining SOF and SOW;
- Failure to define, identify and apply Enhanced Due Diligence in a timely manner, particularly SOF and SOW, to PEPs and other high risk policyholders, for example:
  - No assessment or rationale provided as to why a policyholder was categorised as a PEP rather than high risk;
  - Limited or no additional CDD completed as warranted by the risk profile of the policyholder;
- There were limited or no audit trails maintained to evidence that screening for PEPs and FS had been conducted at onboarding for customers, where manual screening processes were employed.

When a firm is assessing its CDD obligations in relation to new policyholders, the Central Bank expects:

- Firms to demonstrate that they have fully assessed and documented all ML/TF risks to evidence that the application of any exceptions as prescribed by the CJA 2010 is appropriate and the circumstances where exceptions may no longer apply e.g. PEPs;
- Policies and procedures that have regard to the risk based application of CDD, with Enhanced Due Diligence being applied to products and policyholders deemed to be higher risk, as appropriate;
- Policyholder, beneficial owner and beneficiary ID&V procedures to be embedded within the operational processes of the firm;
- Documented evidence to support the application of Simplified Customer Due Diligence ("SCDD") by the firm;

- Firms to ensure that they have effective policies and procedures in place for the identification and management of PEPs, including timely senior management sign off of the PEP relationship;
- Policies and procedures which provide a clear definition of and guidance as to the level of assessment and verification required for the SOF and SOW;
- Appropriate audit trails are maintained of the results of manual PEP and FS screening processes.

3.2 IDENTIFICATION & VERIFICATION OF EXISTING POLICYHOLDERS

Section 33(1)(d) of the CJA 2010, requires that firms adopt CDD measures prior to carrying out any service, where there are reasonable grounds to doubt the veracity or adequacy of documents or information previously obtained for the purpose of verifying the identity of the customer or where firms have not obtained any other information or documentation that can reasonably be relied upon to confirm the identity.

In assessing the firms' application of their requirements under this section of the CJA 2010, the Central Bank found that some firms failed to demonstrate the justification for placing reliance on historic documentation or information held for legacy policyholders, for example:

- In some instances, there was limited, inconsistent or no CDD documentation on pre-2010 sample files reviewed during inspections;
- Limited evidence of consideration or assessment undertaken by the firms in respect of their pre-2010 policyholders ("back book"). Firms were solely relying on trigger events across all product lines without considering whether a more proactive approach was required in certain circumstances. This was a particular concern in respect of medium and high risk product or policyholder categories, or for example in cases where the product features permit the ultimate beneficiary of the policy to differ from the original policyholder;
- Trigger events in place for the purposes of updating CDD varied in robustness and were considered too infrequent to ensure CDD was updated in a timely manner, often only captured at the claim stage of the policyholder relationship.

When a firm is assessing its CDD obligations in relation to existing policyholders, the Central Bank expects that:

- Firms can demonstrate that they have assessed their back book and developed a framework in order to meet their obligations under Section 33 of the CJA 2010. Such a

framework should outline the circumstances and rationale where the firm is satisfied that:

- They can meet their obligations by placing reliance on existing documentation and/or information held on file to identity and verify the policyholder, until such time as a trigger event occurs;
- Exceptions provided for under the CJA 2010 are appropriately applied, with the risk of ML/TF considered and decisions documented;
- Circumstances are defined and documented where a more proactive approach to updating CDD documentation and/or information may be required, as warranted by the risk of ML/TF;

- Firms have developed and implemented a robust trigger events framework which will provide sufficient opportunities to request documentation or information which meets the requirements under Section 33 of the CJA 2010, where any deficiencies have been identified. The following are examples of trigger events which could be utilised. However, this list is not exhaustive and firms must consider all triggers which could be utilised for this purpose:
  - A policyholder seeks a new product or service;
  - A policy has been inactive for a certain period of time and the policyholder makes contact to reactivate;
  - The firm's risk assessment places the policyholder or product in question into a higher-risk category;
  - Any alterations/assignments sought by policyholders to their policy e.g. change of name, change of address, change to policyholders/beneficiaries etc.;
  - Any money movements e.g. top ups, premium adjustments, encashments etc.;
- Firms ensure that they have effective policies and procedures in place documenting their approach and supporting rationale;
- Firms regularly review any measures adopted to determine if updating of CDD, where required, is progressing at an acceptable pace and determine if further process enhancements are required.

3.3 ON-GOING MONITORING OF POLICYHOLDERS

Section 54(3)(c) of the CJA 2010, requires that designated persons adopt measures to keep documents and information relating to customers up-to-date. Firms must document and adopt a risk-based approach to defining refresh cycles to determine the frequency at which CDD information must be renewed. The CJA 2010 also requires that where an existing policyholder becomes a PEP, the measures required by Section 37 of the CJA 2010 must be applied, namely that the business completes Enhanced Due Diligence ("EDD") and obtains senior management approval to continue the relationship with the policyholder.

In addition Section 35(3) of the CJA 2010 requires a designated person to monitor their dealings with a customer by scrutinising transactions and the SOW or SOF for those transactions to determine whether or not the activities of the customer are consistent with the designated person's knowledge of that customer or the purpose and intended nature of the business relationship.

The Central Bank identified the following inadequate practices in operation around the on-going monitoring of policyholders:

- On-going customer and transaction monitoring policy and procedures in place were not sufficiently detailed e.g. lacked detail regarding the setting of parameters to determine the levels and frequency of review and scrutiny required, relevant to the associated risk of ML/TF;
- Firms not adhering to their own internal policies and procedures and risk assessment regarding the on-going monitoring of their policyholders e.g. no evidence to support that specific or sufficient monitoring is conducted on key risk areas identified in the firm's own risk assessment;
- Trigger events were not sufficiently robust to ensure that policyholder documentation and/or information is updated as required by Section 54(3)(c);
- Firms have not fully considered, documented or taken appropriate action in relation to policyholders who have failed to provide the required or updated CDD documentation or information, in line with Section 33(8) and their own policy and procedures;
- Procedures lacked clarity on how to handle the identification and approval process for continuing a relationship with a newly identified PEP e.g. SCDD no longer applies etc.;
- Over reliance on manual systems for the monitoring of transactions.

When a firm is assessing its CDD obligations in relation to the on-going monitoring of policyholders, the Central Bank expects that:

- Firms ensure they have effective and appropriate on-going monitoring policies and procedures in place which are adhered to, including full review and consideration of all trigger events associated with their policyholders;
- Firms ensure that their transaction monitoring programme is risk based, fully documented and are able to demonstrate that the appropriate level of scrutiny has been undertaken;
- Firms ensure they review the data parameters and monitoring reports produced, on a periodic basis, to determine if they are adequate and fit for purpose;
- Firms ensure that there is sufficient assurance testing conducted of their monitoring processes;

- Policyholders re-categorised as PEPs are subject to senior management approval and the completion of EDD;
- Policies and procedures clearly outline the action required where appropriate CDD documentation or information is not held on file, including the various steps that may be taken to locate or obtain such documentation or information should it be necessary to do so.

3.4 RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE

Under Section 40(3) of the CJA 2010, a firm can rely on certain relevant third parties to complete CDD measures required under Section 33 or 35(1) of the CJA 2010. This is often referred to as 'Third Party Reliance'. A written arrangement must be in place confirming that the relevant third party accepts being relied upon and that the relevant third party will provide any due diligence documents or information obtained, as soon as practicable, upon request. However, under Section 40(5) of the CJA 2010 a firm that relies on a relevant third party to apply a measure under Section 33 or 35(1) of the CJA 2010 remains liable for any failure to apply the measure.

In assessing the firms' reliance placed on such third parties, the Central Bank found a number of inadequate practices including:

- Firms had entered into third party reliance arrangements where not all the conditions of Section 40 of the CJA 2010 were being adhered to, for example:
  - Reliance placed on third parties in the absence of a formal reliance arrangement being in place;
  - Inadequate form and content of written third party reliance agreements.
- Lack of or inadequate approved policies and procedures regarding any third party reliance agreements which failed to address areas such as:
  - On-going assurance testing to be completed;
  - Actions to be undertaken in the event of issues identified with or the cessation of a third party reliance arrangement;
  - Appropriate timeframes for the timely transmission of CDD documentation requests by the firm.

When placing reliance on third parties to undertake due diligence, the Central Bank expects that:

- There is a signed agreement in place between the firm and the relevant third party, where the third party has formally consented to being relied on and will, without any

restriction, provide the firm with the underlying CDD documentation and/or information, in a timely manner, upon request;

- The signed agreement must not contain any conditional language, whether explicit or implied, which may result in the inability of the relevant third party to provide the underlying CDD documentation or information upon request;
- Policies and procedures set out an approach with regard to the identification, assessment, selection and monitoring of third party relationships, including the frequency of testing of activity performed by such third parties;
- The firm only relies on the third party to carry out CDD measures required by Sections 33 and 35(1) and not to fulfil on-going monitoring requirements;
- Where a firm routinely relies on checks carried out by a third party, it conducts regular assurance testing to ensure data can be retrieved quickly and without undue delay, that the quality of the underlying documents attained is sufficient and that there are no gaps in policyholder records which cannot be readily explained.

4. IDENTIFICATION AND ESCALATION OF SUSPICIOUS TRANSACTIONS

Section 42(1) of the CJA 2010 requires a designated person who knows, suspects or has reasonable grounds to suspect on the basis of information obtained in the course of carrying on business as a designated person, that another person has been or is engaged in an offence of Money Laundering/Terrorist Financing, to report to An Garda Síochána and the Revenue Commissioners ("the Authorities") that knowledge or suspicion. In accordance with Section 42(2) of the CJA 2010, such a report should be made as soon as practicable.

The Central Bank identified the following inadequate practices in operation around identification and escalation of suspicious transactions:

- Weaknesses in the processes and procedures associated with STRs, including:
  - Deficiencies in internal record keeping;
  - Insufficient or no evidence on files of the assessment and adjudication performed by the MLRO or MLRO delegate on the rationale for discounting suspicions or for making an STR to the Authorities;
  - Staff not receiving an acknowledgment of having raised a suspicion to the MLRO;
  - Unexplained delays in suspicions being reviewed and determined by the MLRO or defined timelines not considered "as soon as practicable"; and
  - Case management of STRs conducted manually by firms, without sufficient audit trails in place to evidence decisions made and actions taken.
- Policies and procedures did not sufficiently outline the internal suspicious transaction reporting process;
- Discrepancies between actual procedures and operational practices e.g. non-use of internal reporting forms;
- No audit trail or on-going monitoring process in place to assist in identifying where ML/TF concerns may have arisen in relation to specific policyholders;
- Lack of assurance testing performed on the STR process.

In relation to the identification and reporting of suspicious transactions, the Central Bank expects that:

- Policies and procedures contain adequate information for employees outlining their obligations to report, as well as guidance on how to sufficiently complete and submit such reports;
- Firms ensure that all STRs are reviewed and reported to the Authorities in a timely manner with evidence of any review retained on file;

- Firms maintain a record of all STRs including details of the investigation and any additional monitoring undertaken;
- If the suspicion is not reported, the details of the assessment and reasons for not doing so should be documented and retained by the MLRO;
- Firms review and validate any monitoring systems and/or reports to ensure that they are meaningful and effective, in particular where transaction monitoring systems generate low levels of alerts;
- Firms ensure that there is an established assurance testing programme in place which includes a review of the STR process for the firm on a periodic basis. Where firms employ a "three lines of defence" model, such testing is included as part of 'third line' assurance testing.

It is important to note that in normal circumstances where a "suspicious" or "unusual" transaction has been identified, a firm may not know whether or not there is an underlying predicate offence. However, in situations whereby the underlying predicate offence is identified, that underlying offence (e.g. theft, fraud, etc.) should be separately reported (in addition to the STR) to An Garda Síochána [Garda Bureau of Fraud Investigation or local Garda Station depending on the nature/complexity of same] to ensure that same can be investigated. If the firm is not the injured party/complainant, then a report pursuant to Section 19 Criminal Justice Act 2011 should be considered in this regard. This is to ensure that An Garda Síochána can investigate the predicate offence as it is precluded from so doing on foot of an STR alone.

5. TESTING OF AML/CFT AND FINANCIAL SANCTIONS IT SYSTEMS

As firms utilise systems in certain areas to facilitate the management and monitoring of Money Laundering/Terrorist Financing and FS risks, it is important that firms take steps to ensure that these systems are operating correctly and effectively. As part of the on-site inspections conducted and the assessment of firms' policies and procedures, the Central Bank conducted a high-level review of the IT processes in place in firms, relating to policyholder onboarding including data management and risk assessment, transaction monitoring, transaction filtering, FS and PEP screening and IT controls.

The Central Bank noted some weaknesses in relation to the IT systems inspected, including:

- Limited automation in monitoring conducted by firms;
- No or limited periodic reviews or controls in place to assess the parameters used and completeness and accuracy of the system generated transaction monitoring reports;
- Absence of system risk ratings to identify products categorised by the firms as high, medium or low risk for the purposes of applying appropriate levels of CDD;
- Limited or no warning notices on systems to assist in recognising and monitoring policyholders identified as PEPs or where previous AML/CFT concerns had been raised.

On the basis of the significant role that systems can play in assisting firms to manage and monitor Money Laundering/Terrorist Financing and FS risks, the Central Bank recommends that firms:

- Consider any system weaknesses identified as part of the refresh of future risk assessments;
- Consider risks when reviewing future system requirements for screening and identification purposes;
- Conduct regular IT assurance testing, as appropriate e.g. controls relating to transaction monitoring such as system parameters to ensure they are operating as anticipated.

6. TERRORIST FINANCING

The offence of Terrorist Financing involves the provision, collection or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism or any act intended to cause death or serious bodily injury. It also includes collecting or receiving funds intending that they be used or knowing that they will be used for the benefit of a terrorist group.

The Criminal Justice (Terrorist Offences) Act, 2005 (the "CJA 2005") gave effect to the 1999 United Nations Convention for the Suppression of the Financing of Terrorism. It created a new offence of financing terrorism and inserted a scheme through which 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.

While financial sanctions are political measures taken to restrict the movement of funds to achieve a specific outcome, Targeted Financial Sanctions are a specific type of financial sanction with a stated objective, one of which is the prevention of Terrorist Financing.

Targeted Financial Sanctions can originate at the supranational level (EU) or international level (UN). While there is a clear obligation to comply with EU Council Regulations, it is also necessary to have regard to the designation of persons and entities by the United Nations Security Council Sanctions Committees ("UN Sanctions Committee(s)") in the Terrorist Financing context. The EU gives legal effect to Targeted Financial Sanction designations by the UN Sanctions Committees through EU Council Regulations.

Once a person or entity is designated by the UN Sanctions Committees, it is intended that funds or other assets are frozen without delay and not made available directly or indirectly to that sanctioned individual or entity. Targeted Financial Sanctions relating to terrorism are dealt with in United Nations Security resolutions 1267 (1999) and 1373 (2001) and their successor resolutions.

While AML/CFT measures are dealt with together in the CJA 2010, it is important to note that a distinction exists in the nature of the two offences of Money Laundering and Terrorist Financing. For Money Laundering to occur, the funds involved must be the proceeds of criminal conduct. For Terrorist Financing to occur the source of funds is irrelevant, i.e. the funds can be from a legitimate or illegitimate source. The key consideration when taking measures to prevent Terrorist Financing is to examine the intended use or destination of the funds as opposed to its origin.

In this regard, the Central Bank expects that:

- Firms take measures to prevent Terrorist Financing and adopt measures to prevent Terrorist Financing commensurate with the risk. The preventative measure for anti-money laundering and combating the financing of terrorism may be the same but will be applied at times in different ways;
- Firms take measures to prevent the financing of terrorism such as carrying out customer due diligence, on-going monitoring, reporting of suspicious transactions, training and having in place effective policies and procedures;
- If a firm has knowledge or a suspicion of Terrorist Financing, it must immediately file an STR;
- In the event that a policyholder, beneficial owner or beneficiary is matched to either the EU terrorist lists or UN terrorist lists, the firm should file an STR immediately with the Financial Intelligence Unit in the Garda Bureau of Fraud Investigation and not carry out any service or transaction in respect of the policy until the report has been made. When the report is made, An Garda Síochána can then take steps and/or give directions to the firm in respect of the policy as appropriate under the CJA 2005 and/or CJA 2010. Where a person or entity is listed in an EU Council Regulation relating to terrorism, there is a legal obligation to immediately freeze that person or entity's account.

7. EU FINANCIAL SANCTIONS

EU Member States implement FS or restrictive measures either autonomously at an EU level, or as a result of binding resolutions of the United Nations Security Council through the adoption of EU Regulations. EU FS Regulations are directly effective and are binding on all EU persons, all entities incorporated or constituted under the laws of the EU and all persons and entities in the EU, including nationals of non-EU countries.

The Minister for Finance gives EU FS Regulations further effect in Irish law by enacting domestic Statutory Instruments (S.I.'s) which provide for the penalties applicable to a breach of the EU FS Regulations. Certain EU FS regulations, such as EU Council Regulation 2580/2001, are specifically implemented for the purpose of preventing the financing of terrorism.

While specific FS requirements vary across FS regimes, the core FS provisions are:

(i) Freezing requirement; freezing action required in relation to all funds and economic resources belonging to, owned, held or controlled by persons, entities and bodies listed in the relevant EU FS Regulation;
(ii) Prohibition on making funds or economic resources available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed in the relevant EU FS Regulation;
(iii) Obligation to notify the Competent Authority; requirement to provide any information in relation to action taken in accordance with an EU FS Regulation or which would facilitate compliance with an EU FS Regulation to the Competent Authority without delay.

Firms must ensure that they have an appropriate framework in place to ensure compliance with all applicable FS Regulations.

In this regard, the Central Bank expects that:

- Firms will devise and implement policies, procedures, systems and controls, to facilitate adherence to their obligations in relation to FS Regulations, for example the implementation of appropriate FS screening mechanisms and procedures for the escalation and management of any potential FS matches;
- Firms will determine the appropriate frequency of on-going screening required, aligned to a documented risk assessment of potential FS exposure.

Firms should also refer to the recently published "Report on Anti-Money Laundering/Countering the Financing of Terrorism and Financial Sanctions in the Irish Banking Sector" for further information on FS Regulations and requirements.

Appendix

Glossary[3]

4th EU Money Laundering Directive	Directive (EU)2015/849. The 4th EU Money Laundering Directive is in response to changes made to the requirements issued by the FATF in February 2012, and a review by the Commission of the implementation of the 3rd EU Money Laundering Directive, issued in October 2005. Member States are required to bring into force the laws, regulations and administrative provisions necessary to comply with the 4th EU Money Laundering Directive by 26 June 2017.
Beneficial Owner	The natural person who ultimately owns or controls the customer. An entity may have more than one beneficial owner.
Beneficiary	The person or entity entitled to receive the claim amount and other benefits upon the death of the insured or on the maturity of the policy.
Central Bank	The Central Bank of Ireland.
CDD	Customer Due Diligence. CDD refers to the range of measures used by designated persons to comply with their obligations under the CJA 2010 in respect of: identifying and verifying the identity of their customers and identifying beneficial owners and verifying their identity; obtaining information on the purpose and intended nature of the business relationship; conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.
CFT	Countering the Financing of Terrorism.
CJA 2010	The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 which came into force from 15 July 2010, transposes the Third Money Laundering Directive (2006/70/EC) into Irish law. The Criminal

[3] All terms contained within this glossary may not be used in the report, but have been included as useful guidance for firms.

	Justice Act, 2013, which amends the CJA 2010 was signed into law on the 12th June 2013. Part 2 of the 2013 Act, which deals with the changes to the 2010 Act came into effect on the 14th June 2013 (with the exception of sections 5, 15 and 16).
Competent Authority	A person or organisation that has the legally delegated or invested authority, capacity or power to perform a designated function.
Designated Person	As defined by Section 25 of the CJA 2010.
EDD	Enhanced Due Diligence. The CJA 2010 requires firms to apply additional, 'enhanced' customer due diligence measures in higher-risk situations. See CJA 2010, Section 37, Section 38 and Section 39.
EU	European Union.
EU Financial Sanctions	Financial sanctions or restrictive measures vary from prohibiting the transfer of funds to a sanctioned country and freezing assets of a government, the corporate entities and residents of the target country to targeted asset freezes on individuals/entities. EU Financial Sanctions may apply to individuals, entities and governments, who may be resident in Ireland or abroad.
FATF	Financial Action Task Force. An intergovernmental body that develops and promotes AML and CFT standards worldwide.
FS	Financial Sanctions. See "EU Financial Sanctions."
ID&V	Identify and Verify. Identification means ascertaining the name of, and other relevant information about, a customer or beneficial owner. Verification means making sure the customer or beneficial owner is who they claim to be.
MLRO	Money Laundering Reporting Officer. The MLRO is responsible for ensuring that measures to combat Money Laundering/Terrorist Financing within the firm are effective. The MLRO should have sufficient AML/CFT knowledge and sufficient seniority, to ensure the independence and autonomy of the role is maintained regardless of

	whether the MLRO also acts as PCF 15, Head of Compliance with responsibility for Anti-Money Laundering and Counter Terrorist Financing Legislation.
MLRO Report	A report prepared at least annually by the MLRO and presented to the Board that analyses and informs on the operation and effectiveness of a Firm's AML/CFT and FS systems and controls established to comply with the CJA 2010.
Money Laundering	The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime.
On-Going Monitoring	The CJA 2010 requires the on-going monitoring of business relationships. This means that the transactions performed by a customer, and other aspects of their behaviour, are scrutinised throughout the course of their relationship with the firm. The intention is to identify where a customer's actions are inconsistent with what might be expected of a customer of that type, given what is known about their business, risk profile, etc. Where the risk associated with the business relationship is increased, firms must enhance their on-going monitoring on a risk-sensitive basis. Firms must also update the information they hold on a customer for AML purposes.
Outsourcing	In the context of this Report, Outsourcing is taken to mean the conduct of activities by a third party service provider, under contract to the firm, where that third party acts as an extension of the firm itself in executing various AML/CFT operational activities.
PEP	Politically Exposed Person. A PEP can be defined as a person who is, or has at any time in the preceding 12 months been, entrusted with a prominent public function. The CJA 2010 also stipulates that the term PEP only applies to non-resident PEPs, i.e. PEPs residing outside of Ireland. This definition is extended to include family members and known close associates of a PEP. PEPs are subject to EDD as per Section 37 of the CJA 2010.

Policyholder	The owner of an insurance policy, usually, but not always, the insured. i.e. the customer of an insurance firm.
REQ	Central Bank of Ireland Risk Evaluation Questionnaires. REQs are completed by firms and submitted to the Central Bank for assessment. REQs facilitate an analysis by the Central Bank of Money Laundering/Terrorist Financing risk through an evaluation of the inherent risk posed by the firm's business model as well as the firm's AML/CFT Control Framework.
SCDD	Simplified Customer Due Diligence. For certain categories of customer or business defined in the Act under Section 34 of the CJA 2010, a set of SCDD measures may be substituted for full CDD, to reflect the accepted low risk of money laundering or terrorist financing that could arise from such business. SCDD does not represent a total exemption as, prior to applying SCDD, designated persons have to conduct and document appropriate testing to satisfy themselves that the customer or business qualifies for the simplified treatment, in accordance with the definitions and criteria set out in the CJA 2010. Designated persons do not have any discretion to add to the categories specified in the CJA 2010 to which SCDD may be applied.
SLA	Service Level Agreement. Should be in place when a firm is using a third party to perform CDD.
SOF	Source of Funds. SOF is required to be provided prior to the approval of a non-resident PEP and may also be required to the extent warranted by the risk of Money Laundering or Terrorist Financing. For SOF, firms should seek to discover the origin and means of transfer for funds that are involved in the transaction.
SOW	Source of Wealth. SOW is required to be provided prior to the approval of a non-resident PEP and may also be required to the extent warranted by the risk of Money Laundering or Terrorist Financing. For SOW, firms should seek to discover the activities that have generated the total net worth of the customer.

Specified Product	As defined by Section 34 (7) (a), (b) & (c) of the CJA 2010.
STR	Suspicious Transaction Report. A report made to the authorities about suspicions of money laundering or terrorist financing. This is also known as a Suspicious Activity Report or SAR. Both terms have substantially the same meaning.
Terrorist Financing ("TF")	An act that constitutes an offence under section 13 of the Criminal Justice (Terrorist Offences) Act 2005.
Third Party Reliance (Section 40)	'Third Party Reliance' as detailed in section 3.4 of this report, relates specifically to the provisions of Section 40 of the CJA 2010, which permits that a designated person may rely on a 'relevant third party' as defined under Section 40 of the CJA 2010, to apply certain measures, only as they relate to Section 33 and Section 35(1) of the Act. Note: these reliance arrangements are separate and distinct from outsourcing arrangements with 'third party service providers'.

T +353 1 224 6000 F +353 1 671 6561 www.centralbank.ie enquiries@centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Bosca PO 559, Sráid an Dáma, Baile Átha Cliath 2, Éire
PO. Box No 559, Dame Street, Dublin 2, Ireland