



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

2015

**Report on Anti-Money Laundering/Countering
the Financing of Terrorism and Financial
Sanctions Compliance in the Irish Funds Sector**



Contents

| | |
|--|-----------|
| 1. OVERVIEW | 2 |
| 1.1 INTRODUCTION | 2 |
| 1.2 BACKGROUND | 2 |
| 1.3 METHODOLOGY | 2 |
| 1.4 SUMMARY OF ISSUES IDENTIFIED | 4 |
| 1.5 CONCLUSION | 4 |
| 2. GOVERNANCE & COMPLIANCE | 6 |
| 2.1 BUSINESS-WIDE ASSESSMENT OF MONEY LAUNDERING/TERRORIST FINANCING RISK | 6 |
| 2.2 OUTSOURCING | 7 |
| 2.3 ROLES & RESPONSIBILITIES | 8 |
| 2.4 POLICIES & PROCEDURES | 9 |
| 2.5 TRAINING | 10 |
| 3. CUSTOMER DUE DILIGENCE | 11 |
| 3.1 ON-BOARDING CUSTOMERS | 11 |
| 3.2 ON-GOING MONITORING OF CUSTOMERS | 13 |
| 3.3 RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE | 14 |
| 4. IDENTIFICATION AND ESCALATION OF SUSPICIOUS TRANSACTIONS | 16 |
| 5. TERRORIST FINANCING | 18 |
| 6. EU FINANCIAL SANCTIONS | 20 |
| Appendix: Glossary | 22 |

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 Funds and Fund Service Providers (each a “Firm” and together the “Firms”) in Ireland.

The Report is based on on-site inspections carried out by the Central Bank over the course of 2014, supplemented by Risk Evaluation Questionnaires (“REQs”) completed by Firms and submitted to the Central Bank for assessment. The Report is based on a sample of Funds and Fund Service Providers operating in Ireland. While all of the issues outlined below did not arise in any one Firm, they are representative of issues identified across all the Firms included as part of the review.

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.

Compliance with the CJA 2010 is a legally enforceable obligation, breaches of which may be 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 components

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:
 - Risk assessment;
 - Outsourcing;
 - Governance structures;
 - Policies, processes and procedures;
 - Management information;
 - Internal Controls;
 - Training.
- Customer Due Diligence (“CDD”), including:
 - Initial customer due diligence;
 - On-going customer due diligence;
 - Reliance on third parties.
- Politically Exposed Persons (“PEPs”) processes for new and existing investors.
- Suspicious Transaction Reporting, including:
 - Process for identification and escalation of suspicious transactions;
 - Decision making process and documentation of rationale for onward reporting to the authorities or not.
- EU Financial Sanctions.

The on-site component of the inspection included the following actions:

- A review of relevant policies and procedures, risk assessments and Management Information (“MI”);
- Interviews with key senior staff, including the Money Laundering Reporting Officer (“MLRO”);
- Sample testing of CDD documentation or information, Suspicious Transaction Report (“STR”) records, third party and outsourcing arrangements, transaction monitoring records and training records;
- Testing of IT systems and controls, including the testing of measures relating to screening of investors for persons subject to FS regulations.

OFF-SITE

The on-site inspections were supplemented by REQs completed by Firms and returned to the Central Bank for review. 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.

1.4 SUMMARY OF ISSUES IDENTIFIED

The issues identified, which are set out in more detail in the remainder of the Report, include:

- Insufficient evidence that the requirements of the CJA 2010 were implemented and that an adequate risk assessment were performed in a timely manner;
- A lack of oversight from the Firm of service providers carrying out AML/CFT functions on behalf of the Firm;
- Reliance on third parties to conduct elements of CDD in circumstances where not all the conditions set out in Section 40 (4) of the CJA 2010 have been fully met;
- Insufficient evidence of effective on-going monitoring of investor transactions;
- Insufficient documentation being retained to support the application of simplified customer due diligence ("SCDD");
- A lack of procedures and controls for ceasing the provision of services to, or discontinuing business relationships with, investors who have failed to provide the required or updated CDD documentation or information requested by Firms;
- Weaknesses in the suspicious transaction reporting processes and procedures and the record keeping associated with these reports;
- Deficiencies in the on-boarding process of PEPs, including the failure to sufficiently identify, verify and document Source of Funds ("SOF") and Source of Wealth ("SOW");
- Insufficient evidence that new PEPs (and existing investors re-categorised as PEPs) are subject to senior management approval and the completion of enhanced due diligence ("EDD");
- Insufficient evidence that all members of the Firm's board and/or staff at the Firm had received instruction in the law relating to AML/CFT issues;
- Documented policies and procedures not being adhered to in all cases.

1.5 CONCLUSION

The Central Bank expects a Fund and its Fund Service Provider(s) to work closely with each other to ensure that appropriate measures are in place to mitigate the risk of Money Laundering/Terrorist Financing. While the Central Bank acknowledges that satisfactory processes and controls were found in some areas, the number and nature of issues

identified suggest that more work is required by Firms in Ireland to effectively manage Money Laundering/ Terrorist Financing risk. While the Funds 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 Money Laundering/Terrorist Financing. 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 Funds sector is a significant part of the Irish financial services industry, both in terms of assets under administration and in terms of the number of investors in Irish funds or funds under the administration of Irish Fund Service Providers. The international reach and scale of these Firms underscore the importance of a high quality risk assessment, which allows Firms to inform themselves of, and to mitigate and manage, all relevant categories of risk. In assessing the approach taken by Firms to conducting risk assessments, the Central Bank identified a number of inadequate practices, such as:

- The risk assessment process is a one-off or ad-hoc exercise and is not used to inform the Firm's risk appetite and/or the need to update policies, procedures and mitigating controls.
- Risk assessments are not reviewed and approved periodically and risk categories (such as country/geographic risk, investor risk etc.) are not reviewed in line with business changes or developments.

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

- Firms undertake and document a Money Laundering/Terrorist Financing risk assessment of their business, to include all risk categories (such as geographic risk, product/service risk, investor risk and channel/distribution risk).
- The underlying methodology, assumptions and risk ratings used are documented.
- Appropriate controls are devised to mitigate any risks identified and that these controls are aligned to and embedded in operational procedures.

- The assessment identifies gaps, with action plans to address such gaps and also identifies the parties responsible for undertaking the resulting actions.
- 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 Money Laundering/Terrorist Financing 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, investor risk and channel/distribution risk).

2.2 OUTSOURCING

While a Firm may outsource certain parts of its AML/CFT activities, the Firm remains ultimately responsible for ensuring compliance with the CJA 2010 and any outsourced service providers are viewed as an extension of the Firm. A Firm must therefore have in place appropriate AML/CFT outsourcing arrangements that ensure all activities are carried out in compliance with the CJA 2010.

When assessing the appropriateness of AML/CFT outsourcing arrangements, the Central Bank found a number of inadequate practices, including:

- The Board of the Firm having limited oversight of the Money Laundering/Terrorist Financing risk managed by outsourced service providers carrying out AML/CFT functions on behalf of the Firm.
- Firms not conducting a full review of the outsourced service provider's AML/CFT policy and procedures.
- A lack of MI provided to Firms by outsourced service providers on AML/CFT issues and a lack of sufficient quantitative and qualitative information available to the Boards of Firms.
- The functions carried out by outsourced service providers are not being regularly monitored through assurance testing, for example through requests for a representative sample of CDD documentation or information to test quality and reliability.
- No documented evidence to suggest that the Firm had obtained evidence that all staff undertaking AML/CFT activities on behalf of the Firm have received appropriate AML/CFT training.

In assessing the AML/CFT outsourcing arrangements in place the Central Bank expects that:

- Firms have appropriate oversight of outsourced service providers carrying out AML/CFT functions, notwithstanding whether the outsourced service provider is a related group entity or comes from outside the group.
- Oversight of outsourced service providers would include the review of the outsourced service provider's policies and procedures and appropriate assurance testing of any AML/CFT functions performed e.g. transaction monitoring processes, suspicious transaction reporting processes and processes to ensure appropriate approval of high risk investors.
- Suitable quantitative and qualitative data is reported to the Board of the Firm by the outsourced service provider to allow an informed view of risks and trends, including reports on the functions carried out by the outsourced service provider and regular MI.
- Firms ensure that all staff undertaking AML/CFT roles on behalf of the Firm are instructed on the law relating to Money Laundering/Terrorist Financing and are provided with on-going training.
- AML/CFT functions are appropriately resourced to perform their roles efficiently and effectively and are subject to regular monitoring and review, for example by Internal Audit.

2.3 ROLES & RESPONSIBILITIES

The Board is ultimately responsible for ensuring compliance with the CJA 2010. Firms must ensure appropriate AML/CFT structures that reflect the nature and complexities of the Firm's relationships and activities are in place. When assessing the Governance structures in place, the Central Bank found a number of inadequate practices, including:

- Limited Board oversight of Money Laundering/Terrorist Financing risk and in particular a lack of oversight of service providers carrying out AML/CFT functions on behalf of the Firm.
- A lack of sufficient MI provided to Boards on AML/CFT issues and a lack of sufficient quantitative and qualitative information included in MLRO reports.
- The resources dedicated to AML/CFT compliance presented difficulties in completing appropriate assurance testing of systems and controls alongside day to day duties.

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

- A Firm's Board can demonstrate active engagement in the monitoring and management of Money Laundering/Terrorist Financing risk, including involvement in the completion

of a Money Laundering/Terrorist Financing risk assessment and continuing consideration of industry developments that may impact the business.

- A Firm has access to the necessary capabilities to ensure the appropriate oversight of service providers carrying out AML/CFT functions, including the review of policies and procedures and assurance testing of the AML/CFT functions performed.
- MI and MLRO Reports provided to the Board, include suitable quantitative and qualitative data to provide (i) an informed view on the performance of the functions carried out by service providers and (ii) an understanding of risks and trends.

2.4 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:

- Implementation of the CJA 2010 and the performance of an adequate risk assessment were not completed in a timely manner and are not subject to regular review.
- Documented policies and procedures were not being adhered to in all cases e.g. triggers to update CDD were not being observed.
- Policies and procedures in place did not cover all of the Firm's obligations under the CJA 2010 e.g. identifying and updating dormant accounts (inactive investors)¹, the process for acquiring senior management sign off of PEP relationships or ceasing the provision of services to, or discontinuing business relationships with, investors who have failed to provide the required or updated CDD documentation or information requested by Firms.

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

- Have a clearly defined process in place for the formal review and approval, at least annually, of the policies and procedures at appropriate levels.
- Risk assessments are reviewed on a frequent basis, at least annually, and are actively used to inform the Firm's risk-based approach and the design of AML/CFT controls.

¹ The term 'dormant accounts' used in the context of the Report, refers to accounts that have been inactive for a period of time, as opposed to zero-balance accounts. The term should not be confused with 'Dormant Accounts' as defined by the Dormant Account Acts 2001 and 2012.

- Policies and procedures demonstrably comply with all legal and regulatory requirements.
- Have appropriate procedures and controls in place to ensure compliance with all aspects of Section 33(8) of the CJA 2010 for investors that have failed to provide adequate CDD documentation or information.
- Have effective policies and procedures in place for the management of PEPs, including procedures for carrying out EDD and for obtaining senior management sign off of PEP relationships. The policies and procedures should also outline timelines for senior management sign off and indicate the seniority of sign off required.

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:

- Not all Board members engaged in on-going AML/CFT training.
- Firms were unable to provide evidence that they had satisfied themselves that staff at outsourced service providers who perform AML/CFT functions on their behalf had received adequate AML/CFT training.

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

- Firms ensure that all persons involved in the conduct of the business (including staff at outsourced service providers) are instructed on the law relating to Money Laundering/Terrorist Financing and are provided with on-going training.
- Adequate training records for all staff are retained.

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”) investors and, where applicable, the beneficial owner(s), prior to the establishment of a business relationship or the carrying out of a transaction or service.

However Sections 33(5), (6) and (7) of the CJA 2010, offer specific exceptions to the general rule established in Section 33(2) or (4) of the CJA 2010. The exception available in Section 33(5) may be used where a Firm has reasonable grounds to believe that verification of an investor’s identity would interrupt the normal conduct of business and where the Firm believes there is no real risk of Money Laundering or Terrorist Financing. The Central Bank found the exception offered by Section 33(5) of the CJA 2010 to be frequently used within the Funds sector. The Central Bank also found the use of this exceptional approach to verification in the Funds sector to be more common than the use by credit institutions and insurance firms of the similar exceptions offered by Sections 33(6) and (7) of the CJA 2010.

In all cases where the exceptional approach to the general rule established in Section 33(2) or (4) of the CJA 2010 is taken, Firms must be mindful of the consequential obligations in Section 33(8) of the CJA 2010. Section 33(8) of the CJA 2010 requires a Firm, who is unable to apply the measures specified in subsection (2) or (4) in relation to a customer, as a result of any failure on the part of the customer to provide the Firm with documents or information required under this section to:

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

3.1 ON-BOARDING CUSTOMERS

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

- Appropriate evidence to support the application of SCDD not being retained on file.
- SCDD being applied to investors who do not meet the definition of a specified customer as prescribed under Section 34 of the CJA 2010 e.g. SCDD being applied to wholly owned subsidiaries of specified customers.
- Firms are not obtaining sufficient information and documentation to fully identify beneficial owner(s).

- Firms are not retaining adequate control over the sign off of new PEP relationships in circumstances where the on boarding of new investors has been outsourced.
- SOF and SOW are not adequately and separately documented.
- Firms have not established adequate procedures for ceasing the provision of services to investors who have failed to provide the required or updated CDD documentation or information.
- An absence of separate and distinct procedures for discontinuing business relationships with investors who have failed to provide the required or updated CDD documentation or information.
- The blocking of additional subscriptions to a Fund, incorrectly being considered to be the discontinuation of a business relationship, for the purpose of Section 33(8)(b).
- Notifications to the investor that the business relationship would be discontinued should they fail to provide the required documentation and/or information did not outline a definitive timeframe in which the Firm would take this action.
- Firms are not taking action on such investors who have failed to provide the required or updated CDD documentation or information, in line with Section 33(8)(b), i.e. discontinuing the business relationship with the investor.

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

- Policies and procedures that set out how additional CDD should be applied to investors in line with increasing or heightened risk.
- Investor and beneficial owner ID&V procedures to be embedded within the Firm and detailed operational requirements for on-boarding established.
- Evidence to support the application of SCDD to be contained on the investor file.
- Firms to ensure that they have effective policies and procedures in place for the management of PEPs, including senior management sign off of the PEP relationship.
- Firms, when scrutinising the SOF, to seek to discover the origin and the means of transfer of the funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends) and when scrutinising the SOW, to seek to discover the activities that have generated the total net worth of the investor (that is, the activities that produced the investor's funds and property).
- Policies and procedures set out the circumstances under which the Firm would cease to provide services or would discontinue an existing business relationship due to an investor's failure to provide the required or updated CDD documentation or information.
- The policies and procedures should outline the process and timeline for ceasing the provision of services.

- The policies and procedures should also include a reasonable, but time bound, programme of contact with the investor and/or or the investor's representative, to afford them the opportunity to provide the required documentation and/or information prior to the discontinuation of a business relationship. The Central Bank expects that before discontinuing the business relationship, Firms will undertake a robust process to obtain the required documentation or information, utilising all available sources.

Policies and procedures should clearly set out the ultimate action to be taken in order to discontinue the business relationship, should the steps taken by the Firm fail to yield the required response from the investor, within the required timeframe.

3.2 ON-GOING MONITORING OF CUSTOMERS

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

The Central Bank identified the following inadequate practices in operation in relation to the on-going monitoring of investors:

- Firms have not implemented policies and procedures to ensure that investor documentation and information is up to date as required by Section 54 (3)(c) and have not outlined possible trigger events associated with these investors.
- Procedures lacked clarity on how to handle the identification and approval process for continuing a relationship with a newly identified PEP.

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

- Firms ensure they have effective on-going monitoring policies and procedures in place including full review and consideration of all trigger events associated with their underlying investors.
- Investors re-categorised as PEPs are subject to senior management approval and the completion of EDD.

3.3 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. An 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:

- The documented arrangements in place between a Firm and a relevant third party not specifically acknowledging that the Firm is relying on the third party to complete CDD measures.
- Documented arrangements in place between a Firm and a relevant third party that contain clauses restricting the provision of such documentation.
- Relevant third parties and arrangements not being regularly monitored through sample testing and assurance testing, for example through requests for a representative sample of CDD documentation or information to test quality and reliability.

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

- 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 documents 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. Examples of such conditional language include (but are not limited to) terms such as *'to the extent permissible by law'*, *'subject to regulatory request'* etc.
- 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 performed on such third parties.
- The Firm only relies on the relevant third party to carry out CDD measures required by Section 33 and 35(1).

- 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 investor records which cannot be readily explained.

4. IDENTIFICATION AND ESCALATION OF SUSPICIOUS TRANSACTIONS

Section 42(1) of the CJA 2010 requires a Firm 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 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 in relation to the identification and escalation of Suspicious Transactions:

- Lack of/no documented policies and procedures for investigating and reporting suspicious transactions identified by directors and/or employees of the Firm, with reliance instead being placed solely on the policies and procedures of the outsourced service provider.
- Weaknesses in the processes and procedures associated with STRs, including deficiencies in internal record keeping, deficiencies in the documenting of the rationale for discounting suspicions or for making an STR, failure to use internal reporting forms, staff not receiving an acknowledgment of having raised a suspicion and unexplained delays in suspicions being reviewed and determined by the MLRO.
- Firms are not reviewing and validating systems that monitor investor transactions to ensure they are meaningful and effective, in particular where systems are generating a low level of alerts.
- Records of on-going transaction monitoring performed are not being retained or are not being fully documented according to the Firm's procedures.
- There was a lack of documented procedures regarding the potential need to report a suspicion in the event that an investor does not provide CDD documentation or information.

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

- 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.
- Policies and procedures contain an adequate description for directors and/or employees of the Firm of their obligations to report a suspicious transaction, as well as guidance on how to complete and submit such reports.

- If the suspicion is not reported, the outcome and reasons for not doing so should be documented and retained.
- Firms have policies and procedures in relation to reporting suspicions that may arise as a result of a failure on the part of the investor to provide the required or updated CDD documentation or information.

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. 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 are 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 have 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 an investor 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 account until the report has been made. When the report is made, the Gardaí can then take steps and/or give directions to the Firm in respect of the account 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.

6. EU FINANCIAL SANCTIONS

EU Member States implement Financial Sanctions (“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 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 and 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

| | |
|---|--|
| 4 th EU Money Laundering Directive | Directive (EU) 2015/849. The 4 th 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 3 rd 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 4 th EU Money Laundering Directive by 26 June 2017. |
| Beneficial Owner | The natural person who ultimately owns or controls the investor. An entity may have more than one beneficial owner. |
| 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 investors 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 Firms' knowledge of the investor, 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 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 14 th 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 and Section 38. |
| 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, an investor or beneficial owner. Verification means making sure the investor 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 an investor, and other aspects of their behaviour, are scrutinised throughout the course of their relationship with the firm. The intention is to identify where an investor's actions are inconsistent with what might be expected of an investor 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 an investor. |
| 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. |
| REQ | Central Bank of Ireland Risk Evaluation Questionnaires. REQ's are completed by firms and submitted to the Central Bank for assessment. REQ's 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 |

| | |
|---------------------|---|
| | <p>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.</p> |
| SOF | <p>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.</p> |
| SOW | <p>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.</p> |
| STR | <p>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.</p> |
| Terrorist Financing | <p>An act that constitutes an offence under section 13 of the Criminal Justice (Terrorist Offences) Act 2005.</p> |



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**