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 Banking Sector

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 banks in Ireland.

The Report is based on on-site inspections carried out by the Central Bank over the course of 2013 and 2014, supplemented by Risk Evaluation Questionnaires ("REQs") completed by Retail and Wholesale banks and submitted to the Central Bank for assessment. The Financial Action Task Force ("FATF") recommends that relevant competent authorities co-ordinate and share information and this Report is also informed in part by the Central Bank's interaction with other competent authorities.

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 a bank operating in Ireland by means of a branch. Consequently, a number of such branches were included by the Central Bank as part of this review.

In performing its role as a competent authority and in preparing the Report, the Central Bank has had regard to recent high profile global AML/CFT and FS developments and international best practices in relation to AML/CFT and FS compliance.

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:
  - Risk assessment;
  - Governance structures;
  - Policies, processes and procedures;
  - Reliance on third parties;
  - Outsourcing;
  - Training;
  - Management information;
  - Internal Controls.
- Customer Due Diligence ("CDD"), including:
  - On-boarding of new customers;
  - On-going monitoring;
  - Correspondent banking.
- EU Financial Sanctions.
- Suspicious Transactions, including:
  - Process for identification and escalation of suspicious transactions.
- Testing of AML/CFT and FS systems.

The inspections, which were carried out over the course of 2013 and 2014, 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");
- On-site walk-throughs of key AML/CFT and FS processes;
- Sample file testing.

OFF-SITE

The on-site inspections were supplemented by REQs completed by Retail and Wholesale banks and returned to the Central Bank for review. 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. In addition the Central Bank co-ordinated with other competent authorities.

1.4 SUMMARY OF ISSUES IDENTIFIED

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

- Incomplete risk assessments that do not effectively consider the inherent Money Laundering/Terrorist Financing risks relevant to the bank;
- The risk assessments undertaken are very high level and lack thorough analysis of key risks;
- Failure to include AML/CFT reviews in annual monitoring and internal audit plans;
- Deficiencies in the Politically Exposed Persons ("PEPs") on-boarding process, including initial screening, the timing of Senior Management approval and the failure to sufficiently identify, verify and document Source of Funds ("SOF") and Source of Wealth ("SOW");
- Non-adherence to stated AML/CFT and FS policies;
- Failure to ensure the provision of appropriate and comprehensive training to Board and committee members, as well as enhanced training for staff in key AML/CFT and FS roles;
- Shortcomings in relation to the coverage and the timing of automated screening of customer databases for FS purposes.

1.5 CONCLUSION

The Central Bank acknowledges that satisfactory processes and controls were found in place in some areas. However, the number and nature of issues identified suggests that more work is required by banks in Ireland to effectively manage Money Laundering and Terrorist Financing risk. While the banking 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 banks 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 banks 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 bank'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 bank's approach to effectively mitigating such risks.

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

The assessment of Money Laundering/Terrorist Financing risk exposure is essential to the effective development of policies and procedures and to a bank's ability to apply proportionate systems and controls. In assessing the approach taken by banks to conducting risk assessments, the Central Bank identified a number of inadequate practices, such as:

- Incomplete risk assessments that do not effectively consider the inherent Money Laundering/Terrorist Financing risks relevant to the bank.
- The risk assessments undertaken are very high level and lack thorough analysis of key risks.
- The risk assessments are not being reviewed and approved periodically, as required by the bank's own internal AML/CFT policies and procedures.
- The risk assessment process is a one-off or ad-hoc exercise and is not proactively undertaken to inform Senior Management of the bank and to inform the risk appetite and/or the policies, procedures and mitigating controls.
- The risk assessment does not adequately record residual risks or identified gaps and does not document the resulting mitigating actions or controls.

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

- The risk assessment includes:
  - The identification and analysis of Money Laundering/Terrorist Financing risks, to include all relevant risk categories (such as country/geographic risk, industry risk, customer risk, product risk and channel/distribution risk).

  - Consideration of all inherent and residual risk factors at country, sector, bank and business relationship levels to inform the design and implementation of policies, procedures and controls that are commensurate with the identified risks.
  - Quantitative data to give an overall inherent risk rating for the bank and its underlying business units, to include sufficient evidence to support the assigned risk ratings.
- The methodology for undertaking risk assessments is documented to ensure consistency across business units, and includes collaborative engagement with the business units to assess risk, to facilitate Senior Management review as well as sign-off and to provide demonstrable engagement at board-level.
- Identified risks are assigned a risk rating having regard to the systems and controls in place to manage those risks.
- The risk assessment identifies gaps with action plans recorded to address such gaps.
- The risk assessment process is driven and overseen by the MLRO and covers all aspects of the CJA 2010.
- Risk assessments are reviewed on a frequent basis by Senior Management and relevant governance committees, at least annually, and are actively used to inform the bank's risk-based approach and the design of AML/CFT controls.

2.2 ROLES & RESPONSIBILITIES

While the Board may delegate its AML/CFT responsibilities to Senior Management, the Board is ultimately responsible for ensuring compliance with the CJA 2010 and must put in place appropriate AML/CFT structures that reflect the nature and complexities of the bank's activities. When assessing the Governance structures in place, the Central Bank found a number of inadequate practices, including:

- The Board and Senior Management take a reactive approach to managing Money Laundering/Terrorist Financing risk.
- Appropriate challenge at formal committee meetings is not evidenced by the relevant meeting minutes.
- Key AML/CFT processes and decisions are contained solely within the respective business units and are not overseen or challenged by the MLRO.
- There is a lack of oversight exercised by banks' Senior Management over key elements of the AML/CFT framework that is outsourced.

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

- The Board has explicitly delineated responsibility for the establishment and management of AML/CFT policies, procedures, systems and controls.
- Senior Management roles and responsibilities are clearly defined and documented.
- There is a clearly established organisational structure that reflects the responsibility for AML/CFT management based upon the nature, size and complexity of the bank.
- The governance structure includes dedicated committees both centrally and at business levels with distinct escalation procedures.
- The Board and Senior Management can demonstrate active engagement in the monitoring and management of Money Laundering/Terrorist Financing risk, including involvement in completion of the Money Laundering/Terrorist Financing risk assessment, effective flows of good quality MI and resulting proactive mitigating actions, 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.
- All relevant parties have formally acknowledged their responsibilities, fully understand their role and are sufficiently senior to have adequate knowledge of the bank, its products, services and systems.
- The MLRO is independent, knowledgeable and provides effective challenge to the business when necessary.
- The AML/CFT unit is adequately resourced.

2.3 POLICIES & PROCEDURES

In accordance with Section 54(1) of the CJA 2010, banks 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:

- Policies and procedures are not subject to regular review or are not reviewed in accordance with the bank's own stated review cycle.
- Reviews are not sufficiently documented to demonstrate the bank has considered whether the current AML/CFT policies and procedures are appropriate and effective to manage the bank's Money Laundering/Terrorist Financing risks.
- Policies and procedures contain out-of-date information or do not reflect actual operating processes.
- Policies and procedures have not been fully implemented across the business units.

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

- Maintain a detailed suite of AML/CFT policies, which are supplemented by guidance and supporting procedures that are tailored by jurisdiction or business unit.
- Have a clearly defined process in place for the formal review and approval, at least annually, of the policies and procedures at appropriate executive and Board committee levels.
- Policies and procedures are readily available to all staff.
- Policies and procedures demonstrably comply with all legal and regulatory requirements.
- Policies and procedures are reviewed in response to events or emerging risks.
- Staff responsible for implementing and monitoring the policies and procedures have adequate levels of expertise and training.
- Policies and procedures are subject to independent review and testing.

2.4 RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE

Under Section 40(3) of the CJA 2010, a bank can rely on certain relevant third parties to complete CDD measures required under Section 33 or 35(1) of 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 bank 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 banks' reliance placed on such third parties, the Central Bank found a number of inadequate practices, including:

- Where third parties are relied upon, those entities do not formally consent to being relied on for CDD checks within a documented and signed agreement.
- The bank's policies and procedures do not clearly define a third party or stipulate whether or when it is acceptable to rely on them.
- The third party is not regularly monitored through assurance testing, for example through requests for sample CDD documents to test quality and reliability.
- A third party who is being relied upon by the bank is unable to retrieve CDD documentation within a reasonable timeline.

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

- There is a signed agreement in place between the bank and the relevant third party, where the third party has formally consented to being relied on and will provide the bank with the underlying CDD information, in a timely manner, upon request.
- The signed agreement requires the third party to provide the bank with CDD documentation or information as requested and permits the bank to undertake a review of control evidence at the third party, as often as may be required, to assess compliance with the CJA 2010 and bank policy.
- 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 bank only relies on the third party to carry out initial CDD measures required by Section 33 and 35(1) and not to fulfil on-going monitoring requirements.
- Where a bank 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 customer records which cannot be readily explained.

2.5 OUTSOURCING

Where a bank outsources part of its AML/CFT responsibilities, the outsourced service provider is viewed as an extension of the bank. Banks must ensure that there is a formal and comprehensive contract or Service Level Agreement ("SLA") in place for all AML/CFT outsourcing arrangements. Under Section 40(7) of the CJA 2010 the bank remains the designated person and is liable for any failure on the part of the outsourced service provider. The Central Bank found that in some instances, contracts/SLAs were not in place for all AML/CFT activities that were outsourced. A documented outsourcing policy should specify the teams or individuals responsible for monitoring and managing outsourcing arrangements and consideration should be given to the impact of expected or unexpected termination of the contract. Banks should also ensure that they have a programme in place for regular testing and verification of the outsourced firm to demonstrate that CDD procedures applied reflect those of the firm.

2.6 TRAINING

Section 54(6) of the CJA 2010 requires banks 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:

- Training records are not maintained showing who had received training, when the training was received, the nature of the training given and the outcome of the training e.g. the results of any assessments.
- Not all Board members completed on-going AML/CFT training.
- Relevant MI e.g. AML/CFT training assessment completion rates, failure rates, etc., is not being generated and circulated to Senior Management.

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

- The training plan is reflective of the levels of Money Laundering/Terrorist Financing risk identified by the bank and is delivered to all staff, including Senior Management and the Board.
- AML/CFT training is provided initially for new hires and at least on an annual basis (or more regularly if required) thereafter for all staff.
- Training content is reviewed and updated on a regular basis to ensure it remains appropriate and the material is signed off by Senior Management.
- Training includes an assessment/exam, which is required to be passed in order for the training to be recorded as completed.
- 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 circulated to Senior Management.

2.7 MANAGEMENT INFORMATION

Under Section 54(1) of the CJA 2010, banks must adopt policies and procedures to prevent and detect the commission of Money Laundering/Terrorist Financing. Section 54(4) of the CJA 2010 requires that banks adopt policies and procedures in relation to the monitoring and management of compliance with, and the internal communication of, the policies and procedures outlined in Section 54(1). In assessing the AML/CFT MI generated, the Central Bank found a number of inadequate practices, including:

- AML/CFT MI reported within business units is not required to be provided to the MLRO, Senior Management or governance committees.
- High level, quantitative MI is being provided but without formal, written commentary to support the analysis of trends and emerging issues.

- No stand-alone MLRO Report is produced, or if produced, it is not presented to the Board and does not include:
  - An assessment by the MLRO as to whether the AML/CFT controls are adequate or require improvement;
  - Details of key actions required by Senior Management;
  - Details of any conclusions or corrective action plans required.

In assessing the AML/CFT MI generated, the Central Bank expects:

- An MLRO Report is produced on at least an annual basis and concludes not only on the effectiveness of the bank's systems and controls but also makes recommendations, as appropriate, for improvement in the management of Money Laundering/Terrorist Financing risk.
- Banks should have regard to the risks presented by its own business model in determining the level and segmentation of MI required. Though not exhaustive, MI should include metrics on the:
  - Number of customer applications declined;
  - Number of customers in respect of which enhanced due diligence was performed;
  - Number of customer relationships terminated due to failure to rectify CDD;
  - Statistics in relation to numbers and types of internal suspicions raised, bases for resolution and statistics regarding the number of external Suspicious Transaction Reports ("STRs") raised.
- MI is regularly produced from an automated process and provided to the most relevant Senior Management and governance committees.
- MI is robust, granular and includes both quantitative and qualitative data to lead to an informed view of risks and trends.
- MI provided ensures good Board and senior level management understanding of not only internal risks but also of emerging, external developments relevant to AML/CFT, new legislation and regulatory developments.
- The suite of MI reporting is regularly reviewed and challenged to ensure that it is fit for purpose and is continually developed when deficiencies are identified.

2.8 LINES OF DEFENCE

Section 54(2) of the CJA 2010 requires that a designated person shall adopt policies and procedures that include an assessment and management of risks of Money Laundering/Terrorist Financing and internal controls, including internal reporting procedures. The Central Bank observed and welcomes that banks operate a "three lines of defence" model to the management and oversight of its Money Laundering/Terrorist

Financing risks. However, during the review the Central Bank found a number of inadequate practices in place around the operation of this model, including:

- The three lines of defence are not properly defined within the organisation, with overlapping AML/CFT functional duties, in particular with regard to the second line performing first line duties.
- Failure to include AML/CFT reviews in annual monitoring and internal audit plans.
- Reviews not conducted on the primary AML/CFT information technology ("IT") systems to ensure the adequacy and appropriateness of the rules and thresholds in operation.

In operating the three lines of defence model, the Central Bank expects:

- An established three lines of defence model with co-ordination between the business unit, Risk, Compliance and Internal Audit to ensure robust and well-structured oversight, as well as effective co-ordination of resources to manage overlap in areas of review.
- The second and third line work plans are prepared using a risk-based approach, with all risks/controls, including AML/CFT, reviewed on a periodic basis.
- Relevant Senior Management and governance committees are involved in the planning of the scheduled reviews and in the closing of findings.
- Testing for specific AML/CFT controls, as well as the overall framework, should be conducted on a regular basis commensurate with the risk.
- Effective, centralised systems should be used to track and monitor issues to resolution.
- Risk, Compliance and Internal Audit units are independent and adequately resourced with staff with knowledge of AML/CFT.

The Central Bank would also expect that cognisance of, and the ability to assess AML/CFT requirements, are considered by banks when selecting external auditors.

3. CUSTOMER DUE DILIGENCE

In accordance with Section 33 of the CJA 2010, banks 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. It should be noted that whilst the definition of a beneficial owner will remain unchanged, the forthcoming 4th EU Money Laundering Directive as currently drafted requires all companies and trusts to hold adequate, accurate and up-to-date information on beneficial owners. Further, to increase transparency, companies and trustees will be required to make this information available to the competent authorities and those conducting AML/CFT due diligence, if requested.

3.1 ON-BOARDING NEW CUSTOMERS

The Central Bank identified the following inadequate practices in operation around the on-boarding of new customers:

- Customer risk ratings and Politically Exposed Persons ("PEPs") markers are not visible to front-line staff.
- Customer risk assessment is based on subjective questions and consequently is susceptible to inconsistency in application.
- Sufficient review of customer and beneficial owner verification documentation is not completed or evidenced by branch managers.
- Directors opening company bank accounts are not being PEP screened. In addition the minutes of board-level committees did not demonstrate that the Board had been informed of, or acknowledged acceptance of, the residual risk arising from not carrying out such PEP screening.
- PEPs can be on-boarded and the account allowed to transact prior to Senior Management approval or Enhanced Due Diligence ("EDD") being complete.
- SOF and SOW are not adequately and separately documented.
- Policies and procedures do not include the requirement to verify, as well as identify, SOF and SOW.
- Failure to apply EDD to high risk customers, including PEPs.

When a bank is assessing its CDD obligations in relation to the on-boarding of new customers, the Central Bank expects:

- Policies and procedures that are risk-based with regard to the application of CDD, with EDD being applied to products and customers deemed to be higher risk.

- Customer and beneficial owner ID&V procedures are established, including detailed operational requirements for on-boarding.
- Policies and procedures that set out the circumstances under which the bank will not accept a new business relationship or would terminate an existing one.
- Consistent understanding of policies and procedures across multiple bank branches.

3.2 ON-GOING MONITORING OF CUSTOMERS

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. Banks 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 customer becomes a PEP, the measures required by Section 37 of the CJA 2010 must be applied, namely that the business completes EDD and obtains Senior Management approval to continue the relationship with the customer.

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

- Procedures providing insufficient guidance on how to identify and action trigger events and failing to clearly set out what customer information is required to be verified and collected upon periodic or event driven reviews.
- Procedures insufficiently documenting a risk-based approach to defining refresh cycles that determine the frequency at which CDD information must be renewed.
- Procedures lacking clarification on how to handle the identification and approval process for continuing a relationship with a newly identified PEP.
- Procedures failing to provide clear guidance in relation to the customer exit process.
- Failure to sufficiently update CDD information and reassess the risk associated on accounts where monitoring indicates material changes to a customer's profile.
- Trigger events that are largely manual, with considerable reliance placed on front-line staff to both identify and action accordingly.
- Insufficient MI escalated to Senior Management in relation to the number of completed and outstanding periodic reviews due for higher risk customers.
- Failure to fully consider the requirements of Section 33(8) of the CJA 2010 in relation to CDD documentation and information. This issue was previously highlighted in the "Dear CEO" letter issued by the Central Bank in October 2012.

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

- The frequency of periodic reviews is commensurate with the level of Money Laundering/Terrorist Financing risk posed by the customer and not based solely upon sales potential.
- Customers are automatically reassessed and, if applicable, re-categorised upon material updates to CDD information and/or other records gathered through a trigger event or periodic review.
- Customers re-categorised as high risk are subject to Senior Management approval and the completion of EDD before a decision is taken to continue the relationship.
- Daily screening of all customers to identify new PEPs is undertaken.
- A well-documented and well-established monitoring programme is in place which is demonstrative of a risk-based approach, where high risk customers are reviewed on a frequent basis.
- Trigger events are clearly defined and understood by staff. The trigger events should be reviewed on a regular basis and revised as required.
- Customer contact is proactively utilised as an opportunity to update CDD information.
- Staff are provided with targeted training on how to undertake periodic reviews and trigger events.
- 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. Where it is necessary to write to customers to seek relevant documentation or information, such communications must clearly detail what is being requested and why, as well as the potential consequences for the customer of failure to provide such documentation or information, as specified in section 33(8) of the CJA 2010.

3.3 CORRESPONDENT BANKING

Section 38 of the CJA 2010 sets out the legislative requirements for on-boarding a new respondent situated outside of a Member State. While the Central Bank observed few new respondent relationships being on-boarded after the introduction of the CJA 2010, the Central Bank did not find evidence that the enactment of the CJA 2010 triggered any review of existing correspondent banking relationships. As the respondent bank is considered to be the customer of the correspondent bank, the on-going monitoring measures required under Section 35(3) of the CJA 2010 must be applied.

Correspondent banking is the provision of a current or other liability account and related services by an Irish based bank (the “correspondent bank”) to another institution situated in a place other than a Member State (the “respondent bank”) to meet its cash, clearing,

liquidity management and short-term borrowing or investment needs. Transactions are processed and executed by the correspondent bank for customers of the respondent. However, the correspondent bank generally does not have direct relationships with the customers of the respondent, as the customer of the correspondent bank is the respondent bank. Due to the inherent structure of this activity and the limited information available in relation to the nature or purpose of the underlying transactions, correspondent banks are exposed to a higher level of Money Laundering/Terrorist Financing risk.

In reviewing correspondent banking arrangements, the Central Bank found a number of inadequate practices in place, including:

- Correspondent banking procedures fail to sufficiently address all requirements of Section 38 and 35(3) of the CJA 2010 e.g. procedures that incorrectly allow for the application of Simplified Customer Due Diligence ("SCDD") to respondents located outside of EU Member States.
- Procedures that do not stipulate what steps should be taken to ensure a respondent is not a shell bank or that the respondent does not have relationships with shell banks.
- Lack of documented responsibilities of the correspondent and respondent bank in applying AML/CFT controls prior to the establishment of the relationship.
- Having no information on file to evidence consideration of adverse information about the respondent or connected individuals, screening of relevant persons for PEP status and FS or site visits to discuss any potential AML/CFT issues.
- Lack of documented Senior Management involvement in, or evidenced approval for, new respondent relationships or existing relationships being reviewed.

With regards to correspondent banking, the Central Bank expects that:

- All respondent relationships are risk assessed and the assigned risk rating drives the level of CDD applied and frequency of relationship reviews.
- The risk assessment of respondent banks takes into account a multitude of risk factors such as the jurisdiction and its AML/CFT regulatory regime; ownership and management structure (including the possible impact or influence of beneficial owners or PEPs); the business purpose of the relationship; operations and transaction volumes; customer base; the quality of the respondent's AML/CFT systems and controls and any negative information known about the respondent or its affiliates.
- Visiting, or at a minimum, liaising with, respondent banks to discuss any potential AML/CFT issues and to gather CDD information.
- The decision to accept or continue a respondent relationship is approved at the senior level of the correspondent bank and the bank can evidence that appropriate

consideration has been given to whether to maintain or exit a relationship. Approvals by Senior Management for all new respondent relationships and for continuance of a relationship must be evidenced.

- On-going monitoring of all respondent relationships is required to be conducted and should be pursuant to the level of Money Laundering/Terrorist Financing risk presented by the relationship. Periodic reviews should be conducted on a regular basis, with higher risk relationships reviewed more frequently, usually annually.
- Regularly screening respondents and connected individuals to identify PEP connections or those on FS lists.
- Automated transaction monitoring should be conducted on the respondent and the underlying transactions.

4. 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.

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.

Banks must ensure that they are in compliance with all current applicable FS. In assessing banks' compliance with EU FS's requirements, the Central Bank's observations are set out below.

4.1 FS POLICIES AND PROCEDURES

While banks had documented FS policies and procedures, the Central Bank observed that in many instances such policies and procedures do not provide sufficient detail to understand the banks' FS compliance programme requirements. FS procedures commonly fail to contain sufficient detail with regard to the grounds for discounting a potential FS match and the level of investigation required for each match. Failing to have prescriptive FS investigation and escalation policies and procedures may result in inconsistencies and a lack of specificity in recorded rationales.

4.2 FS SCREENING

The Central Bank observed that banks had screening processes in place which utilised extensive automation. Generally, new customers were screened overnight following the establishment of the account, with some banks requiring upfront screening of new customers in higher risk business units, such as private banking and capital markets.

In certain circumstances, FS Regulations can require screening of persons and/or entities associated with that sanctioned person. This requirement may arise where the FS Regulation imposes restrictive measures against such persons and/or entities associated (usually where the sanctioned person or entity exercises control over the associated person/entity). The Central Bank found that banks were not always screening persons/entities associated with sanctioned persons.

4.3 FS LIST UPDATES

FS lists updates were commonly sourced from recognised vendors on a daily basis, which automatically updated in the banks' screening solution. Banks predominantly only screened customers daily for changes to FS lists and for changes to client data but none of the banks required or conducted FS screening of the full customer database against the full FS lists on a regular basis. Further, where banks utilised 'Good Guys' lists, an established process for ensuring that the 'Good Guys' was periodically reviewed against updates to the lists had not been implemented.

4.4 FS CASE MANAGEMENT & ESCALATION

Automated case management tools were generally employed for the tracking and resolution of potential matches which adequately maintained evidence of the investigation, including the ultimate decision, rationale and screen prints of evidence reviewed. However, banks commonly failed to sufficiently establish or document agreed service levels for the investigation of potential match investigation and therefore had limited collated MI in relation to screening. Where MI was provided, it lacked statistics on alert volumes, aging of alerts or spikes.

4.5 FS IT ASSURANCE TESTING

The Central Bank found that regular IT assurance system testing of the customer or payments screening solutions was rarely evident. Instead, assurance testing of the effectiveness of the FS lists updates, data feeds and fuzzy logic parameters within the

screening solutions, was conducted on an ad-hoc basis. The Central Bank observed that not all banks policies and procedures clearly defined the IT screening systems or screening solutions testing process and frequency thereof.

The Central Bank expects that banks' FS policies and procedures will address these issues in the future. In addition, the Central Bank expects that the banks' three lines of defence model would incorporate appropriate consideration and review of FS.

5. 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 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:

- Failure to document and implement policies and procedures with regard to the approach for investigating and reporting STRs "as soon as practicable," including the rationale behind the established targets/service level standards.
- Failure to document the process of blocking an account or freezing a transaction on receipt of a court order.
- Lack of comprehensive MI analysis on alerts being generated and reported to Senior Management.
- Inadequate resources in place to effectively meet the volume of alerts and STRs generated.

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

- Policies and procedures contain an adequate description for employees of their obligations to report, as well as guidance on how to sufficiently complete and submit such reports.
- STRs are electronically generated and traced on a case by case basis, assessed and assigned a risk rating and detailed notes are maintained on the decision of whether or not to report to the relevant authorities. Similarly all suspicions reported via the internal reporting process should be electronically recorded.
- The process of investigating and deciding on whether to report a suspicious transaction is completed by a centralised unit to ensure consistency in process and delivery.
- If the suspicion is not reported, the outcome and reasons for not doing so should be documented and retained.

It is important to note that in normal circumstances where a "suspicious" or "unusual" transaction has been identified, a bank 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 bank 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.

6. TESTING OF AML/CFT AND FINANCIAL SANCTIONS SYSTEMS

As banks utilise systems in certain areas to facilitate the management and monitoring of Money Laundering/Terrorist Financing risks and FS, it is important that banks take steps to ensure that these systems are operating correctly and effectively. The Central Bank found that banks only performed limited IT assurance testing on their AML/CFT and FS systems and controls. Generally, the 2nd or 3rd lines of defence were assessing banks' AML/CFT and FS systems and controls for validation of functionality. Where IT assurance testing was conducted, the controls most frequently tested included user access management (access security), batch processing (data uploads/transfers from other systems) and change management (control of configuration changes to the system).

On the basis of the significant role that systems play in the management and monitoring of Money Laundering/Terrorist Financing risk and FS, the Central Bank expects that firms conduct regular IT assurance testing, as appropriate, in relation to:

- General controls relating to the use of automated AML/CFT/FS systems (e.g. system and data access controls, system interfaces, management of system updates, business continuity arrangements).
- Controls relating to transaction monitoring (e.g. review of system parameters to ensure they are operating as anticipated).
- Controls relating to screening and filtering systems (e.g. review of data sources, update and access controls, review of filtering rules and testing to ensure that these rules are operating as anticipated).
- Controls relating to case management systems (e.g. to ensure consistency of reviews and outcomes).
- Controls relating to data sources used to feed AML/CFT and FS systems (e.g. frequency and comprehensiveness of system refreshes).

Appendix

Glossary

4th EU Money Laundering Directive	The proposed 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.
Beneficial Owner	The natural person who ultimately owns or controls the customer. 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 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 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.
Correspondent	Provides a current or other liability account and related services to

Bank	another institution to meet its cash, clearing, liquidity management and short-term borrowing or investment needs.
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."
Fuzzy Matching	The term "fuzzy matching" describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data – whether in official lists or in firms' internal records – is misspelled, incomplete or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process.
"Good Guys" List	A "Good Guys" list is used by banks to reduce the number of false positives by automatically discounting any matches.
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.

IT	Information Technology.
MI	Management information.
MLRO	Money Laundering Reporting Officer. The MLRO is responsible for ensuring that measures to combat Money Laundering/Terrorist Financing within the firm are effective.
MLRO Report	A report prepared by the MLRO and presented to relevant governance committees that analyses and informs on the operation and effectiveness of a bank'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.
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.
Respondent Bank	Receives a current or other liability account and related services from another bank to meet its cash, clearing, liquidity management and short-term borrowing or investment needs.
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 completed when a firm is using another bank, financial institution or third party to perform CDD.
SOF	Source of Funds. SOF is required to be provided prior to the approval of a non-resident PEP.
SOW	Source of Wealth. SOW is required to be provided prior to the approval of a non-resident PEP.
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.

T +353 1 224 6000 F +353 1 224 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