Irish Banks' Obligations Under AML

White Paper – Peadar McCartney

www.DurrusCD.com +(353)-86-8091012 tom.okane@DurrusCD.com

Contents

1 What is Anti Money Laundering?

Anti-money laundering refers to the legislative and regulatory regime for:

- Identifying suspected and known cases of money laundering or the financing of terrorism
- Reporting suspected and known cases of money laundering or the financing of terrorism
- Providing appropriate training to staff to carry out their related statutory obligations
- Record keeping obligations for anti-money laundering processes
- Penalising designated persons for non-compliance with the relevant legislation

The applicable legislation in Ireland is the Criminal Justice (Money Laundering and The Financing of Terrorism) Act 2010, which gives effect to the EU Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and The Financing of Terrorism. The Act is supplemented by a set of related Guidelines issued in 2012 which have been drafted by various sectors of the financial services industry. Whilst these guidelines do not have the effect of law, the Central Bank will have regard to them in assessing compliance with the Act by designated persons. There are several recommendations and guidelines from a range of international bodies including the Financial Action Task Force, an inter-governmental policy making body on financial crime, and the Joint Money Laundering Steering Group in the UK, that are relevant in an Irish context and it is appropriate that persons responsible for implementing anti-money laundering should be familiar with these.

1.1 Banks' Responsibilities

The responsibility for identifying and reporting known or suspected cases of money laundering or the Financing of terrorism rests squarely on several designated persons who may be used as vehicles or innocent facilitators for the legitimisation of the proceeds of financial crime or the financing of terrorist activities.

These designated persons encompass a wide range of businesses, institutions and professionals. For purposes of this paper, we are confining our discussion to the role of banks.

2 Identifying Money Laundering and the Financing of Terrorism

Banks are required to take a risk-based approach to identifying potential money laundering and the financing of terrorism.

An understanding of the risk-based approach is critical to the fulfilment of bank's responsibilities for AML and CFT.

2.1 Risk Based Approach

The risk-based approach recognises that is not possible to monitor every single transaction undertaken by a bank with a view to identifying money laundering or terrorist financing. Adopting a risk based approach implies the adoption of a risk based management process for dealing with money laundering and terrorist financing.
This requires banks to:

- Identify the risks relevant to the bank
- Assess the risks
- Implement measures to mitigate the risks
- Monitor and improve the effectiveness of the mitigation procedures
- Document its overall approach

A risk analysis must be performed to determine where the money laundering and terrorist financing risks are greatest so that the bank can implement proportionate deterrence and detection procedures to prevent the activities from occurring.

There are no prescriptive rules as to how exactly a risk-based approach should be implemented. Banks may choose to operate a low, medium, high assessment or a more complicated scoring system to assess individual risks or combinations thereof. The decision and the appropriate approach in any given case is a question of judgement by senior management in the context of the risks they consider the bank faces.

2.2 Risk Identification, Assessment

The key risks faced by a bank have three components that are to a large degree inter-related. It is necessary to consider the relationship between these risk elements in making an overall assessment of risk in any given situation. The key components are:

- Business Risk
- Customer Risk
- Transaction Risk

2.2.1 Business Risk

Business risk differs in each bank and is a function of the overall profile of the particular bank. Different aspects of the business pose different potential money laundering exposures and their contribution to the institution's risk profile needs to be assessed in order to implement appropriate measures to mitigate the risks that these variables present. It is important to recognise that risk assessment is a dynamic process and that when any of the variables affecting risk are altered, the impact on risk of any change needs to be fully considered.

Some of the variables that require assessment include:

2.2.1.1 Products and Services

Products and services with the highest risk are those where unlimited third party funds can be freely received, or where funds can regularly be paid to third parties, without evidence of identity of the third parties being taken. The product or services could support high-speed movement of funds or along with a high volume of transactions, or both, and could conceal the source of those funds. It may be that the service facilitates a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Consequently, all products and services need to be risk assessed.

2.2.1.2 Geography

Banks operating in countries with an established history of links to terrorism, with a sophisticated financial system and with a substantial presence of international financial institutions are more exposed to money laundering and the Financing of terrorism risk than banks that operate in a less sophisticated environment. In this regard, Ireland, for instance, is considered to be a high risk country from a vulnerability point of view, primarily because of the IRA and the Financial Services Centre in Dublin.

2.2.1.3 Distribution Channels

The use of multiple distribution channels for the provision of products or services increases the risk level. In particular, alternative channels that remove the customer from direct contact with the bank and facilitate a degree of remoteness or anonymity can significantly increase risk. Consequently, services provided exclusively online or through agents require different approaches to risk mitigation than conventional face to face customer interaction.

2.2.1.4 Scale and Complexity

Larger and more complex banking institutions with higher volumes pose higher risks and the procedures and controls implemented in these banks need to be designed take account of the risks that this creates.

2.2.2 Customer Risk

Customer risk is the most significant risk component of money laundering; different customers pose different levels of risk and a clear policy for classifying them into appropriate risk categories is required. Customer risk can only be assessed by applying appropriate customer due diligence investigation, often referred to as "Know Your Customer" (KYC). An effective customer risk assessment should have procedures in place to determine when a customer should not be accepted in order to reduce the risk to the bank.

Know your customer procedures involve the following activities:

2.2.2.1 Establish Customer Identity

The term customer includes the beneficial owner of the account and the first stage in assessing risk is not merely identifying the person who presents themselves as the customer, but also establishing this beneficial owner. The identification required depends on the nature of the customer, specifically whether it is an individual, an institution or an intermediary.

2.2.2.2 Verify Customer Identity

Strict criteria exist for verification of customer identity, depending on the nature of the customer, and whether or not that verification can be carried out by a third party on the bank's behalf. An extensive list of acceptable original documentation is documented in the related guidelines. Particular criteria apply to the identification, verification and acceptance of three special categories of customer, as they are deemed to pose a greater level of risk:

- Non face-to-face customers.
- Politically Exposed Persons – these are non-resident specified senior officials in a foreign jurisdiction.
- Correspondent Banking Relationships - i.e. where the customer is a foreign bank without local operations that is seeking a bank to act on its behalf.

2.2.2.3 Establish Purpose of Intended Nature of Business Relationship

At the outset of a proposed banking relationship, it is important to establish the intended nature of the relationship as this will determine whether the services sought are likely to pose any particular risk to the bank.

2.2.2.4 Establish Source of Income and/or Wealth

The sources of a customer's income or wealth are key factors in assessing potential risk. Income from employment for example is likely to pose a lower risk than income derived from a cash-based business.

2.2.2.5 On-going KYC

Customer circumstances change and it is critical that due diligence is seen to be an on-going activity, as changed circumstances may lead to a change in risk profile. Consequently,

scheduled or trigger-based (e.g. request for services that were originally not envisaged) on-going due diligence is integral to the risk assessment process. Riskier customers require more frequent review.

2.2.3 Transaction Risk

The key to overall risk monitoring is transaction monitoring. The objective is to identify potential incidents of money laundering or the financing of terrorism so that they can be investigated to determine if they warrant investigation and the submission of a suspicious transaction report (STR) to the authorities. The relevant authorities in Ireland are the Fraud Investigation Unit (FIU) of the Garda Siochana and the Revenue Commissioners.

Transaction monitoring is not confined to customers with whom the bank has a business relationship. There is a specific requirement to investigate an occasional transaction for a non-customer where the total amount of money paid in a single or a series of related transactions exceeds €15,000. This requires the bank to conduct due diligence on such a customer before completing the transaction.

The degree of transaction monitoring that takes place is risk-assessed and incorporates the customer risk, the product or service risk and the nature of the transaction itself. In particular, the monitoring process needs to be able to identify whether transactions are consistent with the bank's knowledge of the customer's business and pattern of transactions.

Transaction monitoring focuses not only on flagging transactions that breach defined limits, based on the bank's knowledge of the customer, but also seeks to identify suspicious patterns of activity that may warrant further investigation.

The use of sophisticated analytical tools enables banks to refine transactions, segregating them into ones that pose greater risk for being used as part of a money laundering scheme. In particular, these tools can identify:

1. Unusual fund movements. For example, internal transfers of funds, rapid movement of funds in and out, reactivation of dormant accounts – these are transactions that warrant greater investigation than regular payments in and out of the firm.
2. Unusual behaviours. Frequent changes to the account like changing standing instructions, and leaving excess cash in non-interest bearing accounts can pose additional risk of money laundering.

In recent years, additional analytical tools with the capacity to identify other patterns of behaviour that are consistent with money laundering or the Financing of terrorism have been developed which have greatly enhanced the transaction monitoring process. This is achieved through the use of specially designed algorithms that mine the transaction date with a view to identifying specific typologies or transaction patterns that have been identified in previously discovered money laundering schemes. This has the advantage of potentially identifying

series of small yet related transactions that otherwise might have escaped detection in earlier years as the focus was almost exclusively on transactions that breached a defined financial threshold.

Whilst technology plays a key role in the transaction monitoring process, a substantial degree of reliance is placed on the subjective judgment of staff to identify potential money laundering and terrorist financing. This can only be achieved by having suitably trained staff who are familiar with emerging trends or patterns of behaviour that are indicative of potential money laundering and terrorist financing situations. In this regard, the Financial Action Task Force and many other national and international bodies regularly report on emerging typologies for money laundering and terrorism financing. These typologies are sanitised reports on actual money laundering and terrorist financing schemes that have been detected and can greatly assist people with AML responsibilities in assessing the risks posed by a particular set of circumstances that may not otherwise be detected.

2.3 Sanctions

A separate but related issue to anti-money laundering is the issue of sanctions lists promulgated by the EU and other international bodies. As many of these lists relate to money laundering and the Financing of terrorism, the transactions monitoring processes for anti-money laundering should ideally encompass transaction screening for countries, organisations and individuals detailed on these lists.

3 Reporting Suspected Money Laundering

The reporting of suspected money laundering is a two-stage process – internal and external.

3.1 Internal Reporting

Incidents of suspected money laundering can be the result of automated flagging of certain transactions or suspicions gained by a member of staff. Irrespective of the basis of suspicion, all suspected cases need to be firstly reported internally to a nominated person for further investigation. Each report needs to be fully recorded and documented, outlining the nature of the transactions, the details of the customer and the grounds for suspicion.

Internal reports are then subject to internal scrutiny and examination. Such internal scrutiny and examination will examine not only the underlying transactions, but will also take into consideration the information available from customer due diligence investigation and any other suspicions that may have been previously raised in connection with the customer, irrespective of whether a formal report was made to the authorities. Investigation and scrutiny may require the making of further enquiries either internally, externally or from the customer concerned. Particular care is required at this stage to minimise the risk of alerting the customer or an intermediary that disclosure of the transactions to the authorities is under consideration and there is a specific penalty for the offence of tipping off a person subject to suspicion.

The final determination made as a result of investigation and the reasons therefor should be fully documented and recorded.

3.2 External Reporting

Once the suspected case has been fully examined and a determination made that the activities under investigation constitute valid grounds for suspicion, the Money Laundering Reporting Officer (MLRO) is required to make a Suspicious Transactions Report to the Fraud Investigation Unit of the Garda Siochana and the Revenue Commissioners as soon as practicable after making the determination. The report should include identity of the person suspected, their whereabouts if known and the detailed circumstances giving rise to suspicion. The report may be made by post, fax or encrypted mail.

Once a report has been made, the bank may not proceed with any transaction or service connected with the report unless it is not practicable to delay or stop the transaction or it results in conveying a suspicion to the person under investigation that a report has been or is about to be made to the authorities.

The Garda, on receipt of the STR, may issue a direction to the bank regarding the suspected transactions, failing which the bank may proceed with the transaction. The Act is silent on what is an appropriate time period to wait for directions from the Garda. Additionally, a

District Court judge may make further orders in relation to the suspected customer's accounts.

4 Staff Training

The detection and prevention of money laundering and the Financing of terrorism is dependent on having well-informed trained staff and the Act places an obligation on banks to institute an appropriate training programme for all staff.

4.1 General

All levels of staff need to be aware of the law related to and alert to the risks of money laundering as well as being trained in the various components of the internal processes and controls designed to monitor for, detect and prevent it.

The level and frequency of staff training should be proportionate to their role within the bank.

4.2 Board Level

The obligation to institute appropriate controls to comply with legislation and regulations rests squarely with the Board who are ultimately responsible for the implementation of good governance, risk management and compliance.

Consequently, the Board needs to be trained so that they familiar with and kept up to date with the applicable law, regulations and guidelines and be aware of international developments in the field so that they can fully engage in the decision making processes and take ownership of the risk-based measures adopted.

4.3 Chief Risk Officer

The Chief Risk Officer, subject to Board approval, is responsible for designing the risk-based approach for the bank and therefore requires the greatest level of training.

The key training areas are the legal and regulatory requirements, information on emerging trends and practices and the methodology for implementing a risk-based approach to the detection of suspicious transactions and activity.

4.4 Money-Laundering Reporting Officer

The MLRO needs to be trained concerning the Act and the internal policies and procedures instituted by the bank.

Furthermore, the MLRO needs on-going training on the validation and reporting of suspicious transactions to the authorities and needs to be informed on new trends in criminal activities and related typologies to enable them better fulfil his or her function.

4.5 Customer-Facing Staff

Those dealing directly with customers, except for online banking facilities, are the first point of contact with potential money launderers and terrorist financiers and are critical to the identification of suspicious activities,

Accordingly, they need to be fully trained on their legal obligations and have detailed knowledge of the processes and procedures for the conduct of due diligence on new customers. Furthermore, they need on-going training in relation to factors or transactions that may give rise to suspicion and the procedures for internal reporting of such suspicion.

4.6 New Staff

New staff must have a general appreciation of the background to money laundering and the Financing of terrorism and their personal statutory obligation to report suspicions internally.

5 Record Keeping

The Act lays down detailed requirements for the types of records that need to be maintained, their format, location and the time scale for retention.

The purpose of record-keeping is two-fold:

- To provide documented proof of compliance with the legal and regulatory requirements.
- To facilitate investigation or analysis of suspected money laundering and terrorist activities.

The following is a summary of the key documents that are required to be maintained. The detailed requirements are set out in the Act:

- Records of decisions made on risk policy and the application of the risk based approach.
- Customer due diligence documentation.
- Transaction records.
- Internal and external reports.
- Training records.

6 Penalties

Breaches of any requirements by designated under the Act can lead to fines of up to €5,000 and imprisonment for terms of up to five years.

Additionally, the bank may be subject to administrative sanction by the Central Bank which may result in fines of up to €5m plus the costs of any investigation related to the offence.

These penalties are small relative to the penalties that may be posed internationally which may include a cease and desist order.

www.DurrusCD.com +(353)-86-8091012 tom.okane@DurrusCD.com