

NATIONAL RISK ASSESSMENT FOR IRELAND

Money Laundering
And Terrorist Financing

Executive Summary	1
Background	5
Legal, Judicial and Supervisory Framework	15
Main Threats	24
Financial Services Sector	35
Non-Financial Sector	51
Legal Entities and Arrangements	72
Cash and other Payment Methods	79
Terrorist Financing	87

Executive Summary

1

Objective of National Risk Assessment

This is Ireland's first money laundering and terrorist financing (ML/TF) national risk assessment (NRA), and the aim of this process was to identify, understand and assess the money laundering and terrorist financing risks faced by Ireland. This NRA is also intended to provide the basis for an Action Plan, which, together with the feedback from the FATF Mutual Evaluation Report (MER) and the transposition of the 4th Anti-Money Laundering Directive (4AMLD),¹ will lay the ground for further strengthening the Irish anti-money laundering and countering the financing of terrorism (AML/CFT)² regime.

The Financial Action Task Force (FATF) is an inter-governmental body whose objectives are to set global standards, to promote and to review the effective implementation of legal, regulatory and operational AML/CFT measures. Ireland has been a member of the Financial Action Task Force since 1991. In 2012, the FATF revised the international standards by placing at the core of its forty recommendations a new requirement for countries to identify, assess and understand ML/TF risks particular to their jurisdictions. Ireland is committed to the implementation of the FATF's recommendations which have been endorsed by over 180 countries as the international standards for combating money laundering, countering financing of terrorism, and forestalling the proliferation of weapons of mass destruction.

The requirement to assess risks at country-level is central to the FATF's analysis of the effectiveness of AML/CFT infrastructures. Compliance with many of the remaining recommendations is linked to the quality of the NRA, as the general view is that achieving a clear and comprehensive view of national risks allows countries' policy makers to establish effective multi-agency mechanisms to coordinate domestically on effectively combating identified threats.

The European Union has adopted a similar risk-based approach, and the 4th Anti-Money Laundering Directive will impose obligations on Member States, on the Commission, and on the EU's supervisory agencies to contribute to an ongoing analysis of ML/TF risks at business, country, and EU levels.

Although this is Ireland's first national ML/TF risk assessment, the country's current commitments as a FATF member and its future legal obligations as an EU Member State mean that it will update this assessment on an ongoing basis,³ in order to reflect changes to existing threats and vulnerabilities, and new threats and vulnerabilities as they emerge.

¹ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.141.01.0073.01.ENG

² Where the context permits, references to TF/CFT includes EU and international targeted financial sanctions in relation to terrorist financing and proliferation

³ Article 7(1) – MS “shall keep that risk assessment up to date”

AML/CFT Policy Coordination and Development

Ireland is committed to developing and maintaining a risk-sensitive AML/CFT policy and to further deepening and enhancing the collaboration between domestic agencies and authorities to enhance Ireland's ability to respond to evolving ML/TF risks. A coordinating steering committee, the AML/CFT Steering Committee (AMLSC), has been established to facilitate the collaboration and coordination between national competent authorities, government departments and law enforcement authorities, to ensure the effective combatting of ML/TF.

The AMLSC plays a central role in the development of Ireland's AML/CFT policy and meets on a regular basis. Its objective is to assist Government Departments, agencies and Competent Authorities to fulfil their mandate with respect to measures to combat ML/TF, as provided for in the legislation. The AMLSC's members include the Department of Finance (Chair); the Department of Justice and Equality; the Financial Intelligence Unit; the Criminal Assets Bureau; the Revenue Commissioners; the Department of Jobs, Enterprise and Innovation; the Central Bank of Ireland; and the Office of the Director of Public Prosecutions. Members of the AMLSC are also actively involved in shaping European AML/CFT strategy and policy development, and representatives of members regularly attend international and European meetings, such as the EU's Expert Group on Money Laundering and Terrorist Financing (EGMLTF), which enhances cross-border policy making on AML/CFT; the EU's Supervisory Authorities' Anti-Money Laundering Committee (AMLC) which enhances cross-border AML/CFT supervisory work; the EU's Supranational ML/TF Risk Assessment working group, which enhances and harmonises Member States' ratings of both ML and TF risks; and the EU's FIU Platform Group, Egmont, Europol, and CARIN, which enhances cross-border financial intelligence collaboration.

In addition to the AMLSC, a Cross Departmental International Sanctions Committee (CDISC) has been established to monitor, review, and coordinate the implementation, administration and exchange of information on international sanctions regimes. Government Departments, national competent authorities and other relevant agencies participate in CDISC to discuss emerging issues in this field and to work closely to ensure that Ireland is adopting a coherent and effective approach to the implementation of international sanctions. CDISC's members include the Department of Foreign Affairs and Trade (Chair); the Department of Finance; the Department of Justice and Equality; the Department of Jobs, Enterprise and Innovation; Department of Transport, Tourism and Sport; the Attorney General's Office; the Revenue Commissioners; An Garda Síochána; and the Central Bank of Ireland. Other Government Departments, agencies and other relevant or interested parties may be invited to become a member of CDISC, or to attend certain meetings of CDISC. CDISC's task is to facilitate communication, discussion and the exchange of information between the relevant State authorities in respect of sanctions arising at domestic, EU and international levels. Representatives of the Department of Foreign Affairs and Trade attend the EU's Working Party of Foreign Relations Counsellors (RELEX) committee, which develops and implements the EU's restrictive measures regime, and report on sanctions-related discussions in RELEX to CDISC on a regular basis.

Feeding into the work of the AMLSC and CDISC is the Anti-Money Laundering Private Sector Consultative Forum (PSCF), which has been formed to act as an independent consultative forum, coordinated by the participating private sector representatives, in conjunction with Ireland's preparations for the FATF mutual evaluation review in 2016, and to continue as a consultation forum on AML/CFT issues thereafter. Representatives from the private sector include banks; life insurance providers; payment institutions; funds service providers; investment firms; and designated non-financial businesses and professionals (DNFBPs). The role of the PSCF is to allow stakeholders in the private sector to engage with public agencies to support the development of an appropriate legislative and operational environment, discuss the implementation of AML/CFT measures, develop an understanding of the ML/TF threats, vulnerabilities and risks in the Irish economy, and provide feedback to the AMLSC and CDISC on issues that arise concerning the implementation of the AML/CFT measures.

Overview of the Results of Ireland's First NRA

Taken together, the macro-level risk factors outlined in this section are broadly in balance, and this jurisdiction faces similar risks (neither significantly greater nor lesser) to those faced by other European Member States of similar size. Ireland's ML/TF risk profile is impacted by a number of risk factors at a macro-economic level, including those set out immediately below:

ML/TF risk-enhancing factors:

1. Ireland's economy operates on open, free market principles with a service-exporting financial services sector that, in 2013, was ranked by the IMF among the world's top 29 most interconnected economies,⁴ and was ranked the 5th most interconnected country by McKinsey in 2016.⁵
2. Ireland's membership of the European Union means Ireland subscribes to the four 'fundamental freedoms' guaranteed by European law, hence an economy that had been open to international trade since the 1950s and has, since joining the EEC in 1973, opened further due to the guaranteed freedom to move goods, workers, services, and capital across the internal borders of the Union.
3. Ireland's close economic ties with the United Kingdom and its shared border mean that it could be at risk of certain cross-border activities. Furthermore, the potential impact of the United Kingdom leaving the EU will need to be monitored, particularly with regard to the border.

ML/TF risk-reducing factors:

1. Ireland has a single, centralised police force, An Garda Síochána, which allows it to effectively manage all types of crime. An Garda Síochána is in continuous contact with relevant stakeholders in respect of both ML and TF risk, sharing intelligence as appropriate with vulnerable sectors to assist them mitigate the risks identified later in this report.
2. Ireland has a comprehensive legislative framework criminalising both money laundering and terrorist financing.
3. Ireland has a single, centralised and well-resourced regulator of financial services, the Central Bank of Ireland, reflecting the scale and complexity of the financial sector.⁶
4. Ireland has a single, centralised statistical authority - the Central Statistics Office (CSO) - which publishes annual crime statistics.
5. Ireland's membership of the EU allows it to contribute to and align itself with AML/CFT policy developments along with 27 fellow Member States.
6. Ireland's membership of the EU allows the country to regularly collaborate with other Member States' police forces, FIUs and tax authorities. Increasing levels of collaboration between Ireland and other Member States increases the sophistication of parallel investigative techniques employed by Irish law enforcement agencies (LEAs) in liaison with other Member States and with third countries.
7. Ireland's close relations with its nearest neighbour and largest trading partner, the UK, has allowed the two countries to collaborate effectively to prevent and disrupt economic cross-border crime.

As part of the national risk assessment process, State authorities, private sector representatives, law enforcement agencies, and a myriad of relevant stakeholders were asked to provide their expert knowledge on the levels of ML/TF threats, vulnerabilities, and risks, along with the results of any sectoral risk assessments they themselves had undertaken. These results were then collated, analysed, and discussed further at a number of multilateral workshops, and within the AMLSC, to come up with an overall risk rating for sectors of potential ML/TF risk. These ratings are discussed in detail throughout the report, alongside other relevant areas and developments which were not given a final rating.

⁴ IMF, Press Release: IMF Executive Board Reviews Mandatory Financial Stability Assessments Under the Financial Sector Assessment Program, 13 January 2014, <http://www.imf.org/external/np/sec/pr/2014/pr1408.htm>

⁵ McKinsey, Digital globalization: The new era of global flows, February 2016, <http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>

⁶ The work of the Central Bank of Ireland is discussed further in Chapter 5 – Financial Services Sector

It is important to note, that whilst these ratings are for ‘residual risk’ – i.e. the residual risk after taking mitigants and other relevant factors into account – a higher rating does not necessarily indicate that there is low compliance in this sector. Some sectors will by their very nature or scale remain higher risk even with robust AML/CFT compliance, whilst others may remain relatively unproblematic, despite potential vulnerabilities.

The table below gives a brief overview of the sectors which were given a final risk rating:

Assessed Sector	Rating
Retail Banking	High
Non-Retail Banking	Medium-High
Money Remittance Firms	High
Payment Institutions (other than Money Remitters)	Medium-Low
Bureau de Change	High
Life Assurance	Medium-Low
Funds/Funds Administrators	Medium-High
Asset Managers	Medium-Low
Investment Firms	Medium-High
Credit Unions	Medium-Low
Moneylenders	Medium-Low
TCSPs (Trust or Company Service Providers) (subsidiaries of credit or financial institutions)	Low
Retail Intermediaries	Low
PMCs (Private Members’ Clubs)	Medium-High
HVGDs (High Value Goods Dealers)	Medium-High
TCSPs (Trust or Company Service Providers) (excl. subsidiaries of credit or financial institutions)	Medium-High
Notaries	Medium-Low
PSPs (Property Service Providers)	Medium-Low
Legal Services Sector	Medium-High
Accountancy Services Sector	Medium-High
NPOs (Non-Profit Organisations)	Medium-Low

Background

2

What are Money Laundering and Terrorist Financing?

Money laundering and terrorist financing are global problems that can compromise the integrity and stability of countries' financial systems and institutions. Money laundering is the integration of the proceeds of illegal activity into the legitimate economy and financial sector, with the aim of concealing their criminal origin by making the funds appear otherwise legitimate to others, i.e. the converting of otherwise "dirty" money into "clean" money. By concealing the criminal origin of money, criminals can derive significant personal benefit and can fund further criminality.

Terrorist financing is the collection of funds for distribution to finance domestic and international terrorism. Terrorist financing and money laundering share similarities in the methods used to collect, store and distribute funds, however, in addition to the proceeds of illegal activity, legitimate funds, charities and self-financing may also be used to finance terrorism. The countering of both terrorism and the financing of terrorism is a key priority in ensuring Ireland's security.

National Risk Assessment Purpose, Scope and Methodology

Ireland is committed to combating money laundering and terrorist financing. The purpose of the National Risk Assessment is to provide a broad assessment of Ireland's ML/TF risks to enhance the understanding of them and to develop effective strategies to address them. This assessment is intended to assist the State, its law enforcement authorities, competent authorities, and the public to better understand Ireland's ML/TF risks, so that they can allocate resources and prioritise activities in a proportionate and risk-based manner. Conducting a National Risk Assessment is a key recommendation of the Financial Action Task Force⁷ and is the crucial basis for developing and prioritising AML/CFT policies and activities.⁸ The key findings of this NRA will inform the future development of Ireland's AML/CFT regime.

This assessment is a result of extensive engagement with a wide range of state bodies, supervisors, law enforcement agencies, Ireland's security and intelligence agency, and private sector representatives culminating in an overall collective understanding of ML/TF for the purpose of identifying and assessing the key risks facing Ireland and the effectiveness of Ireland's current approach to addressing those risks. Industry views on ML/TF risks were sought and were used to enhance and substantiate the information provided by the public sector.

Conducting this first NRA exercise also serves to comply with a FATF-aligned requirement of the 4th Anti-Money Laundering Directive; Articles 6-8 of 4AMLD create a special EU framework for ML/TF risk analysis which will operate on three interlinked levels; supranational, between Member States; national, within Member States; and at obliged entity level.⁹ Ireland's NRA has been influenced by and will continue to be influenced by ongoing Supra-National Risk Assessment (SNRA) work at EU level.¹⁰

The results of the national risk assessment will help inform policy and operations and the allocation of resources to the areas of highest risk. It will also help industry in their own risk assessments by giving them

⁷ 2012 FATF Recommendation 1

⁸ 2012 FATF Immediate Outcome 1

⁹ Obligated entity at EU law equates to 'designated person' in Irish AML/CFT law

¹⁰ Article 7.3, 4AMLD

an understanding of the areas of risk where they should have the greatest focus. This is an evolving document which will be updated periodically.

Methodology

The methodology used in the National Risk Assessment was developed having regard to the methodologies developed by other jurisdictions, the FATF guidance, the World Bank and IMF approaches, and extensive consultation with public and private sector stakeholders. The methodology combines qualitative and quantitative information and professional expertise to identify the key risks to Ireland and to develop follow-up actions to address them. A key part of this process is the completion of the AML/CFT Action Plan, following on from the publication of the NRA report, to suggest measures for addressing the risks identified.

The following terms used throughout the National Risk Assessment are defined below:

Threat

Is a person or group of people, an object or activity with the potential to cause harm to the state, society, the economy etc. This includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

Vulnerabilities

When used in a risk assessment, this term comprises those things that can be exploited by the threat or that may support or facilitate its activities.

Consequence

This refers to the impact or harm that ML or TF may cause, and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. For the purpose of this risk assessment, and in line with the methodology of the SNRA, the consequences component is regarded as constantly significant and will therefore not be dealt with in detail. The proposed methodology consequently focus on the threats and vulnerability components.

Mitigants

Mitigants include all circumstances and mitigating measures in place in terms of law enforcement, supervision and capacity to combat ML/TF in various sectors. The mitigants can reduce the overall risk level of a sector where law enforcement and/or supervisory activity effectively mitigates the risk, thus leading to a lower residual risk.

Risk

Risk is a function of threats, vulnerabilities and consequences, as mitigated by certain factors and circumstances. A risk assessment involves making judgements about threats, vulnerabilities, mitigants and consequences.

While there are many similarities between money laundering and terrorist financing in how funds are raised, stored and distributed, the terrorist financing risks posed to Ireland may be somewhat different than those posed by money laundering. For this reason, this assessment includes a separate chapter on terrorist financing.¹¹

Threat, Vulnerability and Risk Identification and Assessment

In order to identify the threats and vulnerabilities relevant to Ireland, a broad range of stakeholders across the public and private sectors were consulted and asked to identify relevant threats and vulnerabilities and to provide quantitative and qualitative information in respect of those threats and vulnerabilities.

¹¹ Chapter 10 – Terrorist Financing

In addition, previously conducted assessments, mutual evaluations, follow-up reports and publicly available academic research were used to identify further threats and vulnerabilities.

The information provided by stakeholders, and otherwise gathered, was considered and assessed by stakeholder experts in multilateral workshops, to identify and prioritise the main threats, vulnerabilities and risks to Ireland. In addition, risk-event scenarios relevant to Ireland were discussed in the multilateral workshops in order to try and enhance the general understanding of risks for the purpose of the NRA.

Moreover, financial sector and non-financial sector Competent Authorities considered the threats, vulnerabilities and risks identified during the multilateral workshops against their independently-conducted sectoral risk assessments. These assessments considered a number of risk factors relevant to those sectors, including amongst others:

- Nature, scale and complexity of the sector;
- Products and services offered by the sector;
- Customers within the sector;
- Distribution channels relevant to the sector;
- Geographical reach of the sector.

The overall findings of the multilateral workshops were analysed and discussed with experts from all relevant stakeholders, and presented to the members of the AMLSC for peer-review, revision where necessary, and sign-off on the final ratings. As such, the findings of this National Risk Assessment are the result of the stakeholders' assessment of the identified risk scenarios supported by qualitative and quantitative data, where available, and is informed by their collective expertise and professional judgment. It is important to note, that whilst these ratings are for 'residual risk' – i.e. the residual risk after taking mitigants and other relevant factors into account – a higher rating does not necessarily indicate that there is low compliance in this sector, as some sectors will by their very nature or scale remain higher risk even with robust AML/CFT compliance, while others may remain relatively unproblematic, despite potential vulnerabilities.

Ireland's Anti-Money Laundering and Terrorist Financing Framework

Irish law relating to anti-money laundering and the countering of the financing of terrorism is set out in the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010, as amended ('the Act' / CJA 2010).¹² The 2010 Act initially transposed the Third Anti-Money Laundering Directive (3AML) and its Implementing Directives, Directives 2005/60/EC and 2006/70/EC, into Irish law, while later amendments in 2013 gave further effect to recommendations of the Financial Action Task Force. The Act requires financial institutions and other designated non-financial businesses or professions to take measures to prevent ML/TF.¹³ Preventative measures set out in Part 4 of the Act include requirements to establish the identity of customers and to report suspicious transactions to Ireland's police-based FIU (within An Garda Síochána). These 'suspicious transaction reports' (STRs) must simultaneously be submitted to both the FIU and the Revenue Commissioners.

In AML/CFT work, STRs can become a key starting point for assessment of sectoral risk, as well as for investigations of suspected money laundering or terrorist financing. It must be noted, however, that a high number of STRs does not necessarily indicate a higher (e.g. high number of suspicious transactions) or lower (e.g. high level of compliance with reporting obligations) risk, but can be a useful tool in AML/CFT policy and enforcement.

¹² Criminal Justice (Money Laundering & Terrorist Financing) Act 2010, <http://www.irishstatutebook.ie/eli/2010/act/6/enacted/en/html> (consolidated version <http://www.betterregulation.com/doc/1/55992>) as amended by Criminal Justice Act 2013, Part 2, <http://www.irishstatutebook.ie/eli/2013/act/19/enacted/en/html> (<http://www.betterregulation.com/doc/1/74119>)

¹³ Section 25, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

Outline of Ireland’s Legislative Framework on Money Laundering and Terrorist Financing

Parts 1 to 3 of the Act define offences of money laundering and terrorist financing and also provide for certain powers for investigation of those offences. Part 4 of the Act provides for the preventative measures that credit and financial institutions and DNFBPs must take in order mitigate risks that their businesses may be abused either to launder illicit proceeds or to finance terrorism. In Ireland, terrorist financing is also criminalised within the anti-money laundering legislative framework, and compliance controls apply equally to both money laundering and terrorist financing.

Offence provisions for substantive laundering under Part 2 of the Act, or for control failures by designated persons under Part 4, are dissuasive. Part 2 offence provisions provide that, on summary conviction, the guilty party could face a fine of up to €5,000 and a term of imprisonment of up to 12 months whereas on indictment, an offender found guilty could be jailed for up to 14 years, or be fined, or both. Under part 4, a 5 year term of imprisonment can be imposed for AML/CFT failures. In the case of credit and financial institutions the Central Bank of Ireland also has significant administrative sanctioning powers.¹⁴

The Act identifies financial and non-financial businesses and professions, defined as ‘designated persons’, which are subject to AML/CFT obligations.¹⁵ Designated persons include:

- Banks
- Payment Institutions,
- Credit Unions,
- Retail Intermediaries,
- Moneylenders,
- Life Assurance Firms,
- Investment Firms and Asset Managers,
- Collective Investment Schemes,
- Funds and Fund Administrators,
- Bureaux de Change and Money Transmission Businesses,
- Independent Legal Professionals (Barristers and Solicitors),
- Auditors, Tax Advisors and External Accountants,
- Trust or Company Service Providers,
- Property Service Providers
- Dealers in High Value Goods (*specifically those who may receive payments in cash of at least €15,000 whether in a single transaction or in a series of linked transactions*), and
- Private Members’ Clubs.

Under the Act,¹⁶ a number of competent authorities are prescribed for the purpose of monitoring the implementation and effectiveness of the measures implemented by the ‘designated persons’ identified by the Act. These competent authorities include, among others, the Minister for Justice and Equality and the Central Bank of Ireland. The competent authorities carry out their supervisory roles through risk-based supervision and employ a range of supervisory measures including, inter alia, desktop reviews and on-site inspections, to monitor AML/CFT compliance within the entities subject to supervision. In addition to complying with the requirements of the legislation, ‘designated persons’ are also legally obliged to report suspicious transactions to both An Garda Síochána and to the Revenue Commissioners.

¹⁴ Part III C of Central Bank Act 1942

¹⁵ Section 25, Meaning of “designated person”, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, <http://www.irishstatutebook.ie/eli/2010/act/6/section/25/enacted/en/html#sec25> (consolidated version) <http://www.betterregulation.com/doc/1/58726>

¹⁶ Section 60, Meaning of “competent authority”, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, <http://www.irishstatutebook.ie/eli/2010/act/6/section/60/enacted/en/html#sec60> (consolidated version) <http://www.betterregulation.com/doc/1/58761>

The Irish anti-money laundering framework was further strengthened by the enactment of the Criminal Justice Act 2013 which amended the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 giving rise to changes in a number of areas including, among others:

- Customer Due Diligence (CDD),
- Requirements for enhanced policies and procedures for detecting and preventing money laundering, and
- Requirements for the retention of documentation overseas (subject to specified conditions).

The Act provides that a number of authorities are responsible for the effective implementation of the AML/CFT framework in the state.¹⁷ The competent authorities are;

- for credit and financial institutions, the Central Bank of Ireland;
- for solicitors, the Law Society of Ireland;
- for barristers, the General Council of the Bar of Ireland;
- for auditors, accountants, tax advisers and certain trust and company service providers, the designated accountancy bodies;
- for high value goods dealers, trust and company service providers, certain tax advisers and accountants, and private members clubs at which gambling activities are carried out, the Minister for Justice and Equality.

AML/CFT Policy Coordination and Development

Ireland is committed to developing and maintaining a risk-sensitive AML/CFT policy. Its approach has been influenced by the FATF recommendations, particularly recommendations 1 and 2. The FATF recommendations require that countries fully understand their risks and collaborate in the development of policies and activities to combat the identified ML/TF risks. Ireland's policy objective in relation to the implementation of AML/CFT is aligned with the FATF's framework. The overarching policy objective is that the *"financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security"*.

In pursuing this high-level objective, Ireland is working towards achieving the following three strategic goals which underpin the national AML/CFT framework;

1. Policy, coordination and cooperation mitigate the money laundering and financing of terrorism risks.
2. Proceeds of crime and funding in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.
3. Money laundering threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. Terrorist financing threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.

Ireland's national AML/CFT policy is evolving in response to national and international issues and emerging trends, to ensure policy is coordinated and communicated effectively. To achieve this, a multi-agency committee structure, with three main components, has been established. This is illustrated in figure 1 on the next page.

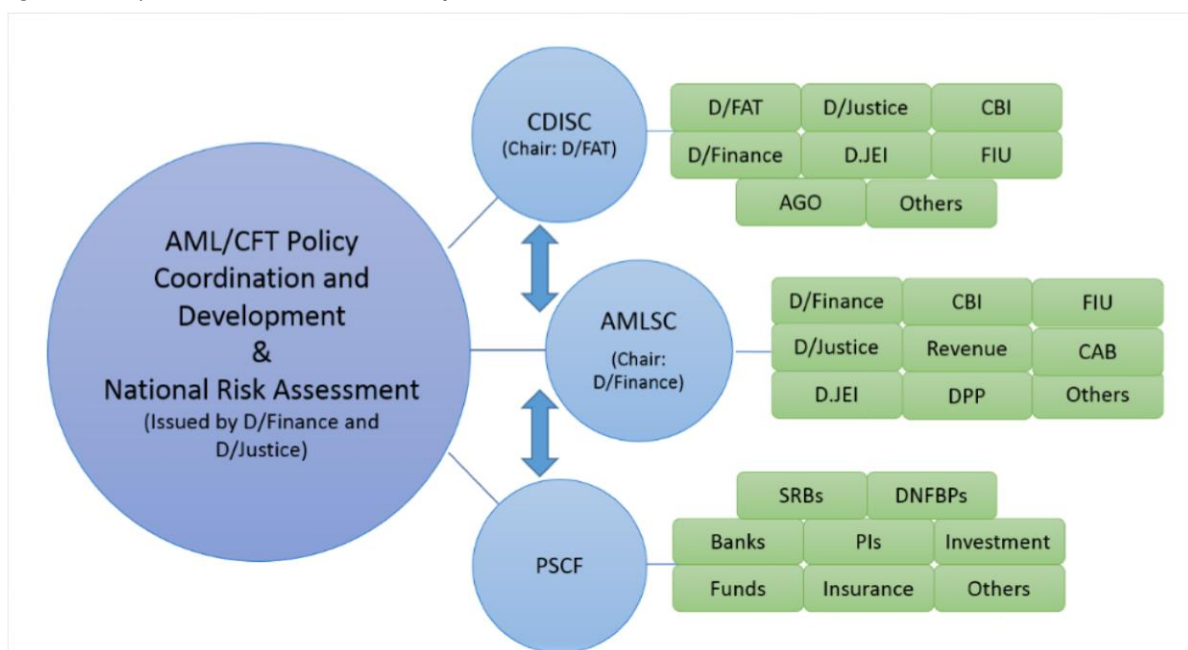
¹⁷ Section 60, Meaning of "competent authority", Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, <http://www.irishstatutebook.ie/eli/2010/act/6/section/60/enacted/en/html#sec60> (consolidated version) <http://www.betterregulation.com/doc/1/58761>

The main components are:

- AMLSC – the AML/CFT Steering Committee;
- CDISC – the Cross-Departmental International Sanctions Committee; and
- PSCF – the Private Sector Consultative Forum.

In addition, the combination of the close collaboration between Ireland’s law enforcement authorities, the unitary nature of Ireland’s police force, and the embedded FIU puts Ireland in a strong position to quickly identify and respond to ML/TF risks as they emerge. This combination, together with the mechanism outlined below, allows Ireland to effectively develop and implement coherent strategies and policies to address those risks with cross-government and cross-industry involvement.

Figure 1: AML/CFT Coordination and Development Structure



AMLSC - AML/CFT Steering Committee

The AML/CFT Steering Committee, or ‘AMLSC’, plays a central role in the development of Ireland’s AML/CFT policy and meets on a regular basis. Its objective is to assist government departments, agencies and competent authorities to fulfil their mandate with respect to measures to combat money laundering and terrorist financing, as provided for in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

The AMLSC’s members include:

- D/Finance, the Department of Finance (Chair);
- D/Justice, the Department of Justice and Equality;
- FIU, the Financial Intelligence Unit;
- CAB, the Criminal Assets Bureau;
- Revenue, the Revenue Commissioners;
- D.JEI, the Department of Jobs, Enterprise and Innovation;
- CBI; the Central Bank of Ireland; and
- DPP, the Office of Director of Public Prosecutions.

The Steering Committee's terms of reference outline its tasks, which are to:

- Facilitate domestic collaboration between members to ensure effective implementation of AML/CFT measures under the legislative framework and international standards;
- Facilitate communication, discussion and feedback between relevant departments, competent authorities, agencies and designated persons regarding developments in international standards and in AML/CFT legislation at EU, national and international levels;
- Identify and agree lead agencies and the areas of competence and responsibility for members under international standards, including the FATF Recommendations, to facilitate a harmonised and effective approach to any reviews that may be conducted by international bodies;
- Facilitate co-operation and collaboration between members in the lead up to international reviews. To agree and coordinate the input of members into a national assessment of the ML/TF risks facing the jurisdiction;
- Coordinate the collective development, by relevant departments, competent authorities and agencies, of national policies to combat money laundering, terrorist financing and the financing of proliferation of weapons;
- Seek to clarify, where necessary, the division of responsibilities between relevant departments, competent authorities and agencies and to establish mechanisms by which they can effectively cooperate with each other on the on-going development and implementation of the above AML/CFT policies;
- Propose and develop measures, such as the gathering of relevant statistics, to establish the effectiveness of initiatives taken by relevant departments, competent authorities and agencies;
- Recommend further initiatives which should be taken to ensure the public is aware of and understands the need for AML/CFT measures; and
- Communicate and collaborate with other relevant inter-departmental/agency committees.

AML/CFT Steering Committee's EU Role

Members of the AML/CFT Steering Committee are actively involved in shaping European AML/CFT strategy and policy development. Members regularly attend international and European meetings of:

- The EU's Expert Group on Money Laundering and Terrorist Financing (EGMLTF) which enhances cross-border policy making on AML/CFT;
- The EU's Supervisory Authorities' Anti-Money Laundering Committee (AMLC) of the Joint Committee of EBA, ESMA and EIOPA, which enhances cross-border AML/CFT supervisory work;
- The EU's Supranational ML/TF Risk Assessment working group, which is responsible for the SNRA which informs the NRA; and

The EU's FIU Platform Group, Egmont, Europol, and CARIN, which enhance cross-border financial intelligence collaboration.

CDISC – Cross Departmental International Sanctions Committee

The AML/CFT Steering Committee is complemented by the Cross Departmental International Sanctions Committee, or ‘CDISC’, whose mandate is to monitor, review and coordinate the implementation, administration and exchange of information on international sanctions regimes. Government departments, national competent authorities and other relevant agencies participate in CDISC to discuss emerging issues in this field and to ensure that Ireland is adopting a coherent and effective approach to the implementation of international sanctions. CDISC is chaired by the Department of Foreign Affairs and Trade (D.FAT). Its members include:

- D.FAT, the Department of Foreign Affairs and Trade (Chair);
- D/Finance, the Department of Finance;
- D/Justice, the Department of Justice and Equality;
- D.JEI, the Department of Jobs, Enterprise and Innovation;
- D.TTAS, the Department of Transport, Tourism and Sport;
- AGO, the Attorney General’s Office;
- The Revenue Commissioners;
- An Garda Síochána; and
- CBI, the Central Bank of Ireland.

The list of members above is not exhaustive. Other Government Departments, agencies and other relevant or interested parties may be invited to become a member of CDISC.

CDISC’s task is to facilitate communication, discussion and the exchange of information between the relevant State authorities in respect of all sanctions regimes, including sanctions relating to terrorist financing and proliferation, arising at domestic, EU and international levels. Representatives of the Department of Foreign Affairs and Trade attend the EU’s Working Party of Foreign Relations Counsellors (RELEX) committee, which develops and implements the EU’s restrictive measures regime, and report on sanctions-related discussions in RELEX to CDISC on a regular basis.

PSCF – the Private Sector Consultative Forum

The AML/CFT Steering Committee is also assisted in its central role by the Private Sector Consultative Forum, or ‘PSCF’, which is intended to allow stakeholders in the private sector to engage with public agencies to:

- Support the development of an appropriate legislative and operational environment so that Ireland has an effective AML/CFT framework in line with international standards;
- Discuss the implementation of AML/CFT measures to ensure compliance with EU law and international standards;
- Develop an understanding of the ML/TF threats, vulnerabilities and risks in the Irish economy;
- Assist in the identification, analysis and review of AML/CFT policies and practices adopted in other jurisdictions; and
- Provide feedback to the AMLSC and CDISC on issues that arise concerning the implementation of the AML/CFT measures.

The PSCF operates a revolving chair, chosen from the members of the forum, who include entities and representative bodies from the financial and non-financial sectors, such as:

- Banks;
- Life Insurers;
- P.I’s, Payment Institutions;
- Funds Service Providers;
- Investment Firms; and
- DNFBNs, Designated Non-Financial Businesses and Professionals

Economic, Geographic, and Political Environment

Economy

Since the late 1950s and, in particular, since becoming a member of the European Union in 1973, Ireland has consistently pursued an economic policy open to international trade and investment. Before joining the European Union, Ireland's economy was largely agricultural-based and closely linked to its nearest neighbour, the UK. Since joining the European Union, and benefiting from the freedoms of membership, Ireland has become increasingly engaged with its European partners and has pursued a deepening of its relationship with the European Union. This relationship is evidenced, in particular, by Ireland's membership of the Eurozone. Through its membership of the European Union, Ireland has grown to become an open, modern, trade dependent economy, with very high levels of import and export trade in both goods and services.¹⁸

Ireland's GDP was approximately €256 billion for 2015,¹⁹ and financial services play an important role in Ireland's open economy. Ireland is the 4th largest exporter of Financial Services in the EU.²⁰ The financial sector brings significant numbers of international financial services companies to Ireland, creating substantial levels of employment and generating significant tax revenue for the State. Overall, over 95,000 people are employed in financial services and other activities,²¹ with over 35,000 of those directly employed by over 400 international financial services companies located in Ireland.²²

Geography

Ireland has a population of approximately 4.6 million people.²³ Ireland has only one land border which it shares with Northern Ireland and it possesses an extensive coastline relative to the population of the country, particularly in the western regions.

These geographical factors may influence the ML/TF threats and vulnerabilities faced by Ireland. Such threats and vulnerabilities may include, for example, cross-border inflows and outflows of physical proceeds of crime and terrorist activities to and from groups in neighbouring countries, regions, or sub-regions. In addition, Ireland's extensive and remote western coastline may make Ireland vulnerable to criminal activities conducted by marine modes of transportation. Law enforcement and customs authorities actively monitor and patrol Ireland's land and maritime borders in close cooperation with European partners.

Given these geographical factors, combating cross-border criminality can be challenging. Ireland cooperates closely and shares intelligence with its European partners to protect the integrity of its land and sea borders. Ireland collaborates particularly closely with UK law enforcement and revenue authorities in detecting and combating criminality across its land border.

Political Environment

Ireland is a sovereign, independent, parliamentary democracy. The National Parliament (the Oireachtas) consists of the President and two Houses: a House of Representatives (Dáil Éireann) and a Senate (Seanad Éireann). The functions and powers of the President, Dáil, and Seanad are derived from the Constitution of Ireland (Bunreacht na hÉireann). All laws passed by the Oireachtas must conform to the Constitution.

¹⁸ CSO, Measuring Ireland's Progress 2014 / Economy / Economy – Finance, <http://www.cso.ie/en/releasesandpublications/ep/p-mip/mip2014/economy/ef/#d.en.96200>

¹⁹ CSO, National Income and Expenditure Annual Results 2015, 12 June 2016, <http://www.cso.ie/en/releasesandpublications/er/nie/nationalincomeandexpenditureannualresults2015/>

²⁰ Department of Finance, IFS2020: A Strategy for Ireland's International Financial Services Sector 2015-2020, March 2015, <http://www.finance.gov.ie/sites/default/files/IFS2020.pdf>, p 9

²¹ CSO, Employment (ILO) (Thousand) by NACE Rev 2 Economic Sector, 'financial, insurance and real estate activities' <http://www.cso.ie/multiquicktables/quickTables.aspx?id=qmq03>

²² Department of Finance, IFS2020: A Strategy for Ireland's International Financial Services Sector 2015-2020, March 2015, <http://www.finance.gov.ie/sites/default/files/IFS2020.pdf>, p 9

²³ CSO statistical release, 26 August 2015, Population and Migration Estimates, <http://www.cso.ie/en/releasesandpublications/er/pme/populationandmigrationestimatesapril2015/>

The Irish legal system is derived from the common law tradition. The Constitution of Ireland, *Bunreacht na hÉireann*, was enacted in 1937 and sets out how Ireland should be governed. The Constitution establishes the branches of government, the courts and also sets out how those institutions should be run.

The country is administratively divided into 26 counties and political power is geographically divided into state, county and municipal levels.

Ireland has been a member of the European Union since 1973.

Corruption

Corruption not only harms proper government and business interests in a country, but also causes significant reputational damage internationally, with consequences for the viability and credibility of economic and government activity. The World Bank has estimated that 1% of global GDP is lost due to corruption and the European Commission estimated that 0.5% of EU GDP is similarly lost. Transparency International ranks Ireland among the 20 least corrupt countries of the 168 countries and territories it monitors.²⁴

Ireland is committed to combating corruption both at home and abroad by establishing and maintaining a transparent and corruption-free environment. In recent years, Irish legislation to prevent corruption, including the Prevention of Corruption Acts, ethics legislation, political funding legislation, money laundering legislation, Lobbying Act, Companies Acts, etc., has been fully brought into line with international standards. Ireland is committed to ensuring that bribes to officials in Ireland and, in certain circumstances, abroad are treated as criminal offences.

The competence to prevent, detect, investigate and prosecute corruption is spread across a number of entities with a mandate to tackle corruption, such as tribunals of inquiry, commissions of inquiry, high court inspectors, the Standards in Public Office Commission (SIPO), local authorities, the Ombudsman, parliamentary committees on members' interests, the Garda Bureau of Fraud Investigation within the police, the Office of the Director of Corporate Enforcement (ODCE), the Comptroller and Auditor-General, the Public Accounts Committee, and the Director of Public Prosecutions.

Codes of conduct are in place for members of Parliament (both Houses) and Office Holders specified under the Ethics Acts. In the local government sector, codes of conduct are in place for Councillors and for local authority employees.

Ireland is a party to a number of international agreements, including the Council of Europe's Group of States against Corruption (GRECO), the United Nations Convention against Corruption, and the OECD Convention on Combating Bribery of Public Officials in International Business Transactions, and has undergone numerous evaluations under these various bodies. The United Nations Convention against Corruption was ratified by Ireland in 2011. This Convention is a comprehensive anti-corruption treaty, providing a set of standards and rules, to encourage countries to strengthen their legal and regulatory regimes to fight corruption, both within the private and public sectors. Its aims are to promote, facilitate and support international co-operation and technical assistance in the prevention of, and fight against, corruption.

The Government has committed to publishing comprehensive legislation on bribery and corruption. The draft schema for the Criminal Justice (Corruption) Bill provides for the consolidation, clarification and strengthening the law criminalising corruption.²⁵ The Bill will replace the Prevention of Corruption Acts 1889 to 2010. The Bill is intended to replace the seven interrelated corruption Acts and to strengthen the penalties applicable on conviction in order to better reflect the damage that corruption does to the economy and to society in general. The draft legislation provides that public officials may be removed from office and excluded from holding office for up to 10 years and where convicted on indictment an offender may be imprisoned for up to 10 years and face a potentially unlimited fine.

²⁴ Transparency International, Corruption Perceptions Index, 2015, <http://www.transparency.org/cpi2015>

²⁵ The general scheme of the Criminal Justice (Corruption) Bill is available at [http://www.justice.ie/en/JELR/Pages/Criminal%20Justice \(Corruption\) Bill](http://www.justice.ie/en/JELR/Pages/Criminal%20Justice%20(Corruption)%20Bill)

Legal, Judicial and Supervisory Framework

3

Ireland has developed a comprehensive and robust legal and institutional framework to combat ML/TF. This framework aims to detect and prevent the proceeds of crime from entering the financial system, and the funding of terrorism. It also aims to deprive criminals of the proceeds of crime, and to punish and deter criminal conduct.

This section of the National Risk Assessment sets out the legal and institutional framework in Ireland and how Ireland's institutions approach the combatting of ML/TF in a coordinated, collaborative and multi-agency manner.

International Framework

The Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body that was established during the G7 summit held in Paris in 1989, in response to the growing threat of money laundering. FATF was formed by the G7 Member States, the European Commission and a further eight countries. FATF's objectives are to set global standards, to promote and to review the effective implementation of legal, regulatory and operational AML/CFT measures. Ireland has been a member of FATF since 1991 and is committed to continuously strengthening its AML/CFT framework to reduce its vulnerabilities in relation to the threat of money laundering and the financing of terrorism.

In 2001, FATF expanded its mandate to include measures to address terrorist financing. FATF has published a series of 40 recommendations which are intended to set out a comprehensive strategy to address global money laundering and terrorist financing in a coordinated manner.

The European Union

The 40 FATF recommendations are incorporated into European law through EU Directives on money laundering and terrorist financing. These FATF-based rules have been tailored to meet the EU's needs and are transposed into national law by Member States. The EU Directives are minimum harmonisation, and accordingly Member States may choose to exceed the provisions of the legislation when they are transposing them into national law. Successive EU Directives have sought to reduce the EU's vulnerability to ML/TF by improving and strengthening the legislative provisions as FATF updates its recommendations and as knowledge of the ML/TF risks to the EU improves. The current EU law on money laundering and terrorist financing is set out in the 3rd Anti-Money Laundering Directive.²⁶ This was adopted at a European level in 2005, after the FATF updated its recommendations in 2004, which also included nine special recommendations on terrorist financing.

After FATF updated its recommendations in 2012, which resulted in the enhancement of the existing global standards, and the European Commission had completed its assessment of the implementation of the 3rd

²⁶ Directive 2005/60/EC of the European Parliament and of The Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Anti-Money Laundering Directive, the 4th Anti-Money Laundering Directive was agreed in June 2015.²⁷ Member States are required to transpose the 4th Directive into national law by June 2017.

The 4th Directive aims to strengthen the European and Member States' AML/CFT frameworks by introducing measures intending to:

- Provide for a focused risk-based approach to supervision and policy development by the EU, Member States, competent authorities and obliged entities;
- Strengthen customer due diligence, or 'CDD', rules;
- Extend the application of enhanced CDD to domestic Politically Exposed Persons (PEPs);
- Lower the threshold for the application of CDD to cash transactions for goods from €15,000 to €10,000;
- Strengthen the cooperation between Member States' financial intelligence units;
- Require companies and trusts to hold information on their beneficial owners; and
- Potentially bring gambling service providers within the scope of AML/CFT measures, subject to a national discretion in this area.

Ireland's Legal and Institutional Framework

Irish law relating to anti-money laundering and the countering of the financing of terrorism is set out in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013. The Act consolidated Ireland's existing AML/CFT legislation and introduced a new and strengthened regime to combat these crimes.

The Act transposed the Third Money Laundering Directive (2005/60/EC) and its Implementing Directive (2006/70/EC) into Irish Law. This brought Irish law into line with EU requirements and also reflected the FATF recommendations. The Act places a number of obligations on certain businesses and professionals to guard against their services being used for money laundering or terrorist financing purposes.²⁸ Such requirements include the obligation to:

- Identify and verify customers and beneficial owners and to apply Customer Due Diligence (CDD) and monitoring measures to those customers;²⁹
- Apply additional measures to customers who are not physically present, politically exposed persons, and to correspondent banking relationships;³⁰
- Report suspicious transactions to An Garda Síochána and the Revenue Commissioners;³¹
- Retain records evidencing the procedures applied, and information obtained, in respect of each customer;³²
- Not "tip-off" any potentially impacted person that a suspicious transaction report has been filed or that an investigation is underway;³³ and

²⁷ Directive (EU) 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

²⁸ Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, Part 4, <http://www.irishstatutebook.ie/eli/2010/act/6/section/24/enacted/en/html#part4> (consolidated version <http://www.betterregulation.com/doc/1/58833>)

²⁹ *Ibid* Sections 33 - 40

³⁰ *Ibid* Sections 37 - 39

³¹ *Ibid* Sections 41 - 47

³² *Ibid* Section 55

³³ *Ibid* Section 49

- Adopt policies and procedures to ensure the effective prevention of ML/TF on a risk-assessed basis.³⁴

In addition, the Act extended the definition of ‘designated persons’³⁵ to include higher risk entities such as trust and company service providers (TCSPs) and private members’ clubs (PMCs). Furthermore, the Act provides for the monitoring of designated persons to ensure compliance with their statutory obligations.

The Act defines the offence of money laundering in terms of property that is the proceeds of crime. Money laundering is committed where a person knows, believes, or is reckless as to whether or not that property is the proceeds of criminal conduct and the person is involved in:

- Concealing or disguising the true nature, source, location, disposition, movement or ownership of the property;
- Converting, transferring, handling, acquiring, possessing or using the property; or
- Removing the property from, or bringing the property into, State.³⁶

The Act describes the proceeds of crime as any property that has been obtained or is derived from criminal conduct in any way, wholly or partly, at any time. The definition of proceeds of crime is broad and captures any form of proceeds that arise from any form of criminal conduct.

The offence of financing terrorism is set out in Section 13 of the Criminal Justice (Terrorist Offences) Act 2005 (‘the 2005 Act’). The 2005 Act gave effect to the 1999 United Nations Convention for the Suppression of the Financing of Terrorism. In addition to creating the offence of financing terrorism it also provides for the freezing and confiscation of funds used, or intended to be used, to finance terrorism.³⁷

Where a person is convicted of money laundering, they are liable on summary conviction to a fine up to €5,000 or up to 12 months imprisonment or both, while on indictment they are liable to an unlimited fine or up to 14 years imprisonment or both, under the CJA 2010.³⁸

Between 2011 and 2015 there were 32 prosecutions for money laundering offences. 29 of those were prosecutions on indictment with 17 secured convictions and 12 outstanding prosecutions. The final 3 prosecutions resulted in summary acquittals.³⁹

The low prosecution rate for money laundering offences, given the increasing numbers of suspicious transaction reports (STRs) being reported,⁴⁰ may be due to difficulties in securing convictions for money laundering compared to securing convictions for the underlying criminal conduct. This is primarily due to difficulties in proving the *mens rea*, intention component of the offence, which is that the person knew or was reckless to the fact that the property was the proceeds of criminal conduct.

Asset Confiscation and Forfeiture

Ireland has implemented a strong and robust confiscation and forfeiture regime to target proceeds of crime in order to deprive criminals of the benefit of those proceeds. Ireland first introduced measures allowing for the seizure and confiscation of the proceeds of crime under the Criminal Justice Act 1994 (CJA 1994), which allowed for the confiscation of assets following a criminal conviction.⁴¹ The CJA 1994 introduced innovative non-conviction, civil measures allowing for the forfeiture of assets without the need

³⁴ *Ibid* Section 54

³⁵ *Ibid* Section 25

³⁶ *Ibid* Section 7

³⁷ Sections 14 – 16, Criminal Justice (Terrorist Offences) Act 2005,

³⁸ Section 7(3), Criminal Justice (Money Laundering & Terrorist Financing) Act 2010, as amended, <http://www.irishstatutebook.ie/eli/2010/act/6/section/7/enacted/en/html#sec7> (consolidated version <http://www.betterregulation.com/doc/1/58708>)

³⁹ DPP submission to AMLSC, March 2016

⁴⁰ 21,700 in 2015, 18,300 in 2014 and 15,200 in 2013. Based on information provided by the FIU

⁴¹ Sections 4, 9, 39, Criminal Justice Act 1994, <http://www.irishstatutebook.ie/eli/1994/act/15/enacted/en/html> (consolidated version <http://www.betterregulation.com/doc/1/24839> and <http://www.betterregulation.com/doc/1/41428>)

for a criminal conviction. The Proceeds of Crime Act 1996 (POCA) also provides for these measures, and are implemented by the Criminal Assets Bureau (CAB) which was also established in 1996.

These measures were introduced in response to a significant growth in organised crime and the emergence of criminals who were not directly perpetrating offences yet enjoyed the benefit of the proceeds of those offences.

As such, Ireland’s criminal justice system provides for two independent regimes to target the proceeds of crime, a criminal confiscation regime, and a civil forfeiture regime. These regimes have a number of similarities which include:⁴²

- Both regimes target all proceeds of crime, whether they are the direct or indirect proceeds, money or property; and
- Both regimes operate using the civil standard of proof,⁴³ which is on the balance of probabilities.

However, the regimes also have a number of differences which include:

- A criminal conviction is necessary for the operation of the criminal confiscation regime; and
- The property the subject of a POCA action must be worth at least €13,000.⁴⁴

In 2014, approximately €460,000 was forfeited to the State under POCA,⁴⁵ and approximately €1,185,000 was confiscated under the CJA.⁴⁶ In addition, CAB successfully froze a further €6,760,000 in assets in 2014.⁴⁷

The recently enacted Proceeds of Crime Act 2016 provides Criminal Assets Bureau officers with the power to seize property which they suspect to be the proceeds of crime and detain it for 24 hours. The Chief Bureau Officer will be empowered to authorise its detention for a further 21 days. This period will allow CAB to prepare an application to the High Court for an interim restraining order and prevent the disposal or dissipation of the property in the meantime. The other key focus of the Act is the threshold value of property which can be pursued by CAB under the Proceeds of Crime Act 1996. It is to be reduced from €13,000 to €5,000. This provision will support the work of the Bureau in targeting the middle value proceeds of crime held by those involved in organised crime.

Criminal Confiscation

The Office of the Director of Public Prosecutions (DPP) established a dedicated Assets Seizing Section in 2007, which co-ordinates and monitors all applications brought under the CJA. The Assets Seizing Unit is in the Solicitors Division of the DPP’s Office.

The criminal confiscation regime provided for by the CJA allows for the confiscation and forfeiture of proceeds of crime where a person has been convicted of an offence. In addition, the CJA reduced the standard of proof that must be satisfied in order to secure an order under the CJA to the civil standard, which is on the balance of probabilities. The standard of proof for obtaining the conviction remains as the criminal standard, beyond reasonable doubt.

Section 4 of the CJA allows for the confiscation of money in the case of a conviction on indictment for drug offences. Once a person has been convicted on indictment of a drug trafficking offence and has been sentenced, the trial court must determine whether the convicted person has benefited from the drug trafficking, the extent to which the person has benefited and the amount that is realisable to discharge a confiscation order. The Court can then make a confiscation order for that amount.

⁴² Savona Ernesto U. & Riccardi Michele (Eds.), 2015, From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Final Report of Project OCP – Organised Crime Portfolio (www.ocportfolio.eu). Trento: Transcrime – Università degli Studi di Trento, p 107 (“OCP”), p 233

⁴³ Sections 4, 9, 39, Criminal Justice Act 1994, <http://www.irishstatutebook.ie/eli/1994/act/15/enacted/en/html> (consolidated version <http://www.betterregulation.com/doc/1/24839> and <http://www.betterregulation.com/doc/1/41428>)

⁴⁴ Section 2, Proceeds of Crime Act 1996, <http://www.irishstatutebook.ie/eli/1996/act/30/section/2/enacted/en/html> (consolidated version <http://www.betterregulation.com/doc/1/54619>)

⁴⁵ Criminal Assets Bureau, Annual Report 2014, p 17

⁴⁶ Office of the Director of Public Prosecutions, Annual Report, p 55

⁴⁷ Criminal Assets Bureau, Annual Report 2014, p 13

Section 9 allows the confiscation, on conviction, of the benefit a person has gained from any indictable offence other than drug trafficking offences. An inquiry may be held by the Circuit Court into the benefit gained after the person is sentenced. The prosecution must prove that the benefit generated is directly related to the offence with which the accused is charged before the court can make any confiscation order.

Section 39 of the CJA 1994 allows for the forfeiture of money seized during a search conducted by An Garda Síochána or Revenue under Section 38 of the CJA 1994, where the Circuit Court is satisfied that the money seized directly or indirectly represents the proceeds of crime.

Finally, Section 24 of the CJA 1994 allows the DPP to apply to the High Court for an asset freezing order where a person is charged, or a decision has been taken to charge that person, with an indictable offence. The freezing order can cover property belonging to an accused person located in Ireland or abroad. Freezing orders are designed to prevent the dissipation of assets prior to a confiscation inquiry being conducted by the trial court if the accused is convicted on indictment of the offence with which they are charged.

Civil Forfeiture

The civil confiscation regime is provided for by POCA and implemented by CAB, whose primary aim is to target the proceeds of crime in Ireland. The objective of the regime is to deprive the holder of property, which derives from criminal conduct, of the beneficial enjoyment of that property. While the criminal confiscation regime acts *in personam*, which is against a convicted criminal, the key difference with the civil confiscation regime is that it acts *in rem*, which is against the property that is the proceeds of crime, rather than against the person. As such, no criminal conviction is necessary for CAB to seek an order under POCA.

In addition, similar to the criminal confiscation regime under the CJA, the standard of proof that must be satisfied in order to secure an order under POCA is the civil standard, which is on the balance of probabilities.

The key remedies available to CAB under POCA are interim orders, interlocutory orders and disposal orders.

Section 2 of POCA allows CAB to apply to the High Court for an interim order to prevent any dealing in property which is valued above €13,000 where the court is satisfied, on the balance of probabilities, that the property is the proceeds of crime. An interim order can remain in place for 21 days.

Section 3 of POCA allows CAB, within 21 days of the granting of an interim order under Section 2, to apply to the High Court for an interlocutory order which allows for the long-term freezing of an asset that is the proceeds of crime for a period of at least 7 years.

Section 4 of POCA allows CAB, 7 years after the granting of an interlocutory order under Section 3, to apply to the High Court for a disposal order which causes the assets to be forfeited and transferred to the State.

While the regime allows for the freezing and forfeiture of assets without proof of criminal conduct on the part of a respondent, the regime also contains a number of safeguards which ensure that the regime is fair and that it is not oppressive or punitive. These include that:

- Persons may challenge orders granted by the High Court to vary their effect or set them aside entirely;
- The High Court may provide for compensation where an order has been shown to be unjust;
- Respondents have access to legal aid; and
- Persons claiming ownership to property have a right to be heard by the Court before a disposal order is granted under Section 4 of POCA.

Law Enforcement Authorities

Overview

Ireland has a unitary national police force, An Garda Síochána, which is responsible for carrying out all policing, security and intelligence duties in the State. This is almost unique amongst common law countries and has the benefit of consistency of approach, single police force, the rapid sharing of information and intelligence between police and security units, the ability to quickly redeploy resources to respond to changing needs and the benefits of economies of scale. In addition, Ireland's unitary policing structure has the significant advantage of being the single point of contact with international counterparts. This enables an efficient contribution to the combating of international crime, money laundering and terrorist financing.

An Garda Síochána is headed by the Garda Commissioner who is accountable to the Minister for Justice and Equality. The Minister is, in turn, accountable to the Dáil, the Irish legislature, in respect of policing and criminal justice matters in Ireland.

As of December 2014, there are approximately 12,800 Gardaí in Ireland,⁴⁸ who are supported by approximately 1,100 Garda Reserves and a further 2,400 civilian staff.⁴⁹

While An Garda Síochána has general responsibility for combating criminal conduct, including predicate offences for money laundering, there are a number of branches of An Garda Síochána which are particularly relevant in combating ML/TF. They are:

- FIU, the Financial Intelligence Unit;
- MLIU, the Money Laundering Investigation Unit;
- C&S, the Crime and Security Branch;
- SDU, the Specialist Detective Unit;
- GBFI, the Garda Bureau of Fraud Investigation;
- DOCB, the Drugs and Organised Crime Bureau;
- GNPSB, Garda National Protective Service Bureau;
- NBCI, National Bureau of Crime Investigation;
- GNIB, Garda National Immigration Bureau;

In addition to these specialist units of An Garda Síochána, the combating of money laundering and terrorist financing in Ireland involves the close collaboration of:

- CAB, the Criminal Assets Bureau;
- Revenue, the Revenue Commissioners;
- DPP, the Office of the Director of Public Prosecutions;
- The Department of Social Protection;
- The Companies Registration Office; and
- The Central Statistics Office.

GBFI - Garda Bureau of Fraud Investigation

The GBFI is a specialist unit of An Garda Síochána that investigates complex and serious fraud including commercial fraud, cheque and credit card fraud, cybercrime, and incidents of counterfeit currency. The GBFI's mandate is to investigate and prosecute fraud and financial crime in Ireland. The GBFI works with other Garda units and state agencies such as the Revenue, the Companies Registration Office, the Central

⁴⁸ An Garda Síochána, Annual Report 2014

⁴⁹ *Ibid*

Bank of Ireland, and the Office of the Director of Corporate Enforcement (ODCE) to fulfil this mandate. The GBFI houses the Money Laundering Investigation Unit (MLIU) and the State's Financial Intelligence Unit.

FIU - Financial Intelligence Unit

Ireland's Financial Intelligence Unit, or 'FIU', is a law enforcement-style financial intelligence unit which is embedded within the GBFI, and is a national reception point for STRs submitted under Irish money laundering legislation.⁵⁰ However, it operates independently and autonomously within the GBFI. As such, it is able to effectively exchange information in respect of STRs it receives, within An Garda Síochána and externally through established information exchange channels.

The FIU analyses and disseminates STRs and intelligence gained, to other national units within An Garda Síochána and Gardai throughout the country for investigation and potential further action. In tandem with this, An Garda Síochána has members on secondment in a number of agencies, such as the Office of the Director of Corporate Enforcement, the Competition and Consumer Protection Commission, and the Department of Social Protection, to which the FIU can share intelligence. The FIU also engages with Revenue in respect of the STRs it receives in order to consider their quality and content, and STRs of mutual interest. This inter-agency collaboration is possible because Ireland operates a dual-reporting system for STRs. Designated persons are required to report suspicious transaction to both the FIU and Revenue.⁵¹ The FIU works closely with the Crime and Security Unit within An Garda Síochána to ensure that any intelligence of interest is shared in a timely fashion and appropriate action is taken. The FIU analyses STRs which have potential domestic or international terrorist financing links.

The FIU has observed a significant increase in the numbers of STRs reported by designated persons in recent years. In 2015, the FIU received almost 21,700 STRs compared to approximately 18,300 in 2014 and 15,200 in 2013.

The FIU actively cooperates with law enforcement agencies in other jurisdictions in matters relating to suspected money laundering and terrorist financing. This includes the exchange of intelligence via FIU.Net, Egmont Secure Web, Interpol and Europol.

The FIU is a member of the Anti-Money Laundering Operational Network (AMON) which is a relatively new initiative consisting of a network of professional investigators working together on cross border investigations into money laundering. AMON is an informal network established with the intention of speeding up formal requests in the area of money laundering investigations. Its aim is to facilitate the exchange of information among investigators and to direct requests to the most appropriate formal channels. FIU Ireland has attended three AMON annual general meetings to date and has appointed two experienced practitioners as contact points for AMON.

The FIU provides training to members of An Garda Síochána throughout the country to create awareness of the value of financial intelligence in the fight against money laundering, terrorist financing and all criminality. In addition, the FIU collaborates with Revenue in delivering industry AML/CFT training to raise the awareness of emerging money laundering trends and typologies, and to provide feedback on the nature and quality of STR reporting to industry. The recent increase in the number of STRs reported to the FIU and Revenue, in particular due to regulatory interventions and sanctioning, has focused the emphasis of industry training on improving quality of STRs reported by designated persons.

MLIU – Money Laundering Investigation Unit

The FIU supports the Money Laundering Investigation Unit, or 'MLIU', within GBFI and it investigates complex money laundering cases and/or cases which have cross-jurisdictional links. It extracts information from the analysis of STRs allowing for the instigation of criminal investigations.

⁵⁰ Section 42, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, <http://www.irishstatutebook.ie/eli/2010/act/6/section/42/enacted/en/html#sec42> (consolidated version) <http://www.betterregulation.com/doc/1/58743>

⁵¹ *Ibid*

Suspected terrorist financing can also be investigated by the MLIU. The MLIU also provides advice and assistance to other members of An Garda Síochána who are investigating cases of suspected terrorist financing.

Crime and Security Branch

The Crime and Security Branch identifies and analyses the threat to the State from terrorists and organised crime gangs. The section deals with intelligence in relation to both terrorism and organised crime; and supports other units of An Garda Síochána by providing intelligence leads relative to both areas.

Specialist Detective Unit

The Specialist Detective Unit is responsible for the investigation of threats to the security of the State security and the monitoring of persons who pose a threat to this on both national and international fronts.

Drugs and Organised Crime Bureau

The Drugs and Organised Crime Bureau is a specialist unit within An Garda Síochána with responsibility for proactively targeting and investigating drug trafficking and serious organised crime both within Ireland and outside the jurisdiction.

Garda National Protective Service Bureau

The Garda National Protective Service Bureau is responsible for investigating sexual crime and human trafficking.

National Bureau of Crime Investigation

The National Bureau of Criminal Investigation was established as an effective and active response to the proliferation of serious and organised crime.

Garda National Immigration Bureau

The Garda National Immigration Bureau is responsible for all law enforcement matters pertaining to immigration. The Bureau monitors the movement of non-nationals at all air and seaports throughout the State and along the border with Northern Ireland, with a view to the prevention and detection of illegal immigration.

CAB - Criminal Assets Bureau

CAB was established by the Criminal Assets Bureau Act 1996 to implement the civil forfeiture regime provided for by POCA. CAB is also empowered to ensure that the proceeds of criminal conduct are subjected to tax,⁵² and to pursue individuals engaged in criminal conduct for social welfare debt.⁵³ CAB adopts a multi-disciplinary and multi-agency model to target the proceeds of crime by bringing together law enforcement expertise from policing, tax, social welfare, legal, forensic, and financial analysis backgrounds to target the proceeds of crime using a “follow the money” approach.

CAB is widely regarded, both nationally and internationally, as a robust and best practice model in the context of combating organised crime. It works closely with international crime investigation agencies, and has successfully targeted proceeds of foreign criminality from countries such as the US and the UK. CAB also works with international bodies such as the European Commission and Camden Assets Recovery Inter-agency Network (CARIN). CARIN is an informal network of law enforcement agencies, who share knowledge and information on how to trace assets in a member country.

⁵² Section 5, Criminal Assets Bureau Act 1996, <http://www.irishstatutebook.ie/eli/1996/act/31/section/5/enacted/en/html#sec5>
(consolidated version <http://www.betterregulation.com/doc/1/54579>)

⁵³ *Ibid*

In 2014, CAB froze €6,760,000 in assets,⁵⁴ secured the forfeit of €460,000 to the State,⁵⁵ recovered approximately €3 million in taxes from 55 individuals and entities,⁵⁶ and recovered social welfare debts of approximately €335,000.⁵⁷

The Revenue Commissioners

Revenue's role is to serve the community by fairly and efficiently collecting taxes and duties and implementing customs controls. Revenue tackles non-compliance across all tax categories, including customs and excise. Non-compliance takes many forms, including failing to make a tax return, tax evasion, and smuggling.

Revenue has a range of tools and techniques at its disposal to tackle non-compliance. These range from light-touch early interventions to criminal prosecutions for serious tax and customs fraud. Revenue uses sophisticated risk-assessment, analytics and intelligence-gathering systems to target interventions for maximum impact.

STRs are processed, evaluated and where possible developed and disseminated to the relevant Revenue region to deal with. In addition STRs are "worked" in order to develop intelligence in support and counter the activities of those involved in tax evasion and smuggling.

Revenue's Financial Intelligence Section (FIS) sits within the Central Investigations Branch of the Investigation and Prosecution Division. The section's remit is to analyse financial intelligence, primarily through exploitation of STRs, and filter this intelligence through the wide range of data sources to support existing investigations and intelligence gathering activity.

In 2014, Revenue secured 27 criminal prosecutions for serious tax and duty evasion.⁵⁸ At year-end 2014 there were 64 cases in the prosecutions pipeline, with a further 115 cases under investigation. In addition, 504 criminal convictions were secured for a range of summary tax, customs and excise offences, as a result of which fines of €1,173,620 were imposed.⁵⁹

Office of the Director of Public Prosecution

The majority of cases dealt with by the Office of the Director of Public Prosecutions, or 'DPP', are received from the Garda Síochána. However, some cases are also referred to the Office by specialised investigative agencies including the Revenue Commissioners, the Health & Safety Authority, the Competition Authority, the Garda Síochána Ombudsman Commission, the Environmental Protection Agency, local authorities and other government departments.

The DPP retains a specialist unit which receives files from investigatory agencies nationwide specifically in relation to anti-money laundering investigations. The Anti-Money Laundering Unit within the DPP works closely with the Asset Seizing Unit of the DPP and other law enforcement agencies.

Between 2011 and 2015, the DPP directed that 32 files received from investigatory agencies should be prosecuted for money laundering offences. 29 of those were prosecutions on indictment with 17 secured convictions and 12 outstanding prosecutions. The final 3 prosecutions resulted in summary acquittals.

⁵⁴ Criminal Assets Bureau, Annual Report 2014, p 13

⁵⁵ *Ibid* p 17

⁵⁶ *Ibid* p 25

⁵⁷ *Ibid* p 28

⁵⁸ Revenue, Annual Report, p 35

⁵⁹ Revenue, Annual Report, p 7

Main Threats

5

Money Laundering Threats in Ireland

This section of the National Risk Assessment sets out the understanding of the nature and scale of criminal conduct in Ireland which generates illicit proceeds, particularly as informed by law enforcement authorities. Ireland's long-standing policy is to pursue parallel investigations into all potential ML/TF activity arising from the predicate offences described below. In pursuing their objectives, Irish law enforcement authorities and statutory bodies responsible for the confiscation of criminal assets, continuously liaise with each other to develop a coherent strategy to target assets and profits derived from criminal conduct, and in particular, from organised crime.

Information in this section is derived from the knowledge and expertise of all Irish law enforcement authorities. Criminal activities considered particularly generative of illicit proceeds are:

- Drug offences;
- Financial crime;
- Tobacco smuggling;
- Tax evasion;
- Prostitution;
- Fuel laundering;
- Theft and burglary;
- Cybercrime;
- Human trafficking;
- Bribery and corruption; and
- Other illicit trade, such as counterfeiting and intellectual property theft.

While Ireland is considered a relatively low crime country,⁶⁰ proceeds-generating criminal conduct, common to all developed economies, is present. Predicate offences are perpetrated by offenders of various levels of sophistication, from small scale criminals, through criminalised professionals to organised crime gangs (OCGs). It is estimated that there are approximately 40 OCGs in Ireland, of which at least 9 have international links with OCGs in regions such as the Netherlands, Spain, West Africa and the United Kingdom.⁶¹ The presence in Ireland of foreign OCGs is evident in multi-jurisdictional economic crime areas such as human trafficking, drugs smuggling and distribution, firearms smuggling, tobacco smuggling, vehicle theft, and counterfeiting, although the extent to which Irish or foreign OCGs control these markets is difficult to estimate. The level of multi-jurisdictional OCG activity in Ireland has increased in recent years, both on a cross-border basis; with OCGs in Northern Ireland, and internationally, where increased collaboration has become evident.

By its nature, it is difficult to gauge the exact scale of proceeds generating criminal conduct. The United Nations Office on Drugs and Crime estimated that 2.7% of global GDP in 2009 was laundered, which is consistent with the International Monetary Fund's previous estimated range of 2-5% of GDP.⁶² Research suggests that the scale of money laundering in Ireland was 1.1% of GDP in 2010 (€1.7 billion).⁶³

⁶⁰ See, for example, OECD Better Life Index - Safety Section <http://www.oecdbetterlifeindex.org/topics/safety/>

⁶¹ Savona Ernesto U. & Riccardi Michele (Eds.), 2015, From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Final Report of Project OCP – Organised Crime Portfolio. Trento: Transcrime – Università degli Studi di Trento, p 107 (“OCP”)

⁶² UNODC, Illicit money: how much is out there?, 25 October 2011, http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-_how-much-is-out-there.html

⁶³ Savona Ernesto U. & Riccardi Michele (Eds.), 2015, From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Final Report of Project OCP – Organised Crime Portfolio, Trento: Transcrime – Università degli Studi di Trento, (“OCP”), p 37

Drug Offences

Drug offences pose the most significant threat of money laundering to Ireland. While there has been a decrease in the numbers of drug offences recorded in recent years,⁶⁴ drug offences still accounted for over 7% of all recorded offences in 2015.⁶⁵ Intelligence suggests that while domestic OCGs are the main perpetrators of drug offences, they are closely linked with international OCGs.

Due to Ireland's extensive coastline and location at the western edge of the European Union it is vulnerable to use as an entry-point for illicit drugs into the EU and as a conduit for onward transit to other EU markets. The international sources for drugs imported into Ireland have been mapped in detail and are well-understood. Law enforcement and customs authorities actively monitor and patrol Ireland's land and maritime borders to detect and seize illicit drugs before they reach the Irish or European market. Close cooperation and intelligence sharing with European partners, and with the Maritime Analysis and Operation Centre-Narcotics (MAOC-N), has prevented significant amounts of illicit drugs entering the Irish or EU market.⁶⁶

In 2014 the Garda National Drugs Unit arrested 60 persons in connection with drug trafficking offences with €698,234,000 of controlled drugs seized,⁶⁷ with approximately €673 million seized as part of strategic drugs investigations in liaison with partners identified above. These seizures would support research suggesting that Ireland is not only a destination but also a strategic transit country for illicit drugs destined for the UK and other EU countries.⁶⁸

In 2014, illicit drugs valued at €91 million were seized in Ireland by the Revenue Commissioners. This compares to €20 million in 2013, €49 million in 2012, €24 million in 2011, €9 million in 2010 and €39 million in 2009.⁶⁹ In 2014 amounts seized by Garda actions alone amounted to approximately €57 million.⁷⁰ As with many figures in this field, seizure values cannot be relied upon as a consistent indicator of overall scale, due to issues with 'outlier' seizures and the generally irregular nature of drugs seizures.

Proceeds from drugs offences are generally cash-based, with law enforcement intelligence suggesting that bulk cash transportation, third party laundering, high value goods dealers, cash-intensive front businesses and gambling are some of the laundering methods commonly used by criminals associated with drug trafficking. However, the emergence of online drug purchasing and the possible use of cryptocurrencies to fund such purchases present new challenges for law enforcement authorities which are being analysed.

⁶⁴ Information furnished to the AMLSC by An Garda Síochána

⁶⁵ CSO, Statistical Product - Recorded Crime,

http://www.cso.ie/px/pxeirestat/DATABASE/Eirestat/Recorded%20Crime/Recorded%20Crime_statbank.asp?sp=RecordedCrime&Planguage=0

⁶⁶ See Garda Annual Report, 2014, p 6, example of 1,025 tonnes of Cocaine seized aboard SV Makayabella in September 2014

⁶⁷ Garda Annual Report, 2014, p 4

⁶⁸ OCP, p 107

⁶⁹ Revenue Commissioners Annual Reports 2009-2014

⁷⁰ Garda Annual Report, 2014, p 42

Financial Crime

Financial crime poses a significant threat of money laundering to Ireland and covers a wide range of traditional and computer-enabled fraud offences perpetrated by a variety of individuals and sophisticated OCGs. Financial crime offences include:

- White-collar crime;
- Social welfare fraud;
- Bogus investment frauds;
- Mortgage fraud;
- VAT/MTIC fraud;⁷¹
- Commercial fraud;
- Phishing;
- Inheritance scams;
- Invoice redirection fraud;
- Payment card fraud;
- Cheque fraud; and
- Card-not-present fraud.

The detection and investigation of fraud offences in Ireland is approached in a multi-agency, multi-faceted, manner by Ireland's law enforcement authorities, who collaborate together to detect, deter, and prevent fraud. The Garda Bureau of Fraud Investigation - GBFI, the Computer Crime Investigation Unit - CCIU, Revenue, and The Department of Social Protection's Special Investigations Unit - SIU, are responsible for the investigation of fraud, social welfare fraud, deception, and computer crime offences in Ireland. In addition, law enforcement authorities actively collaborate with counterparts in the United Kingdom, the European Anti-Fraud Office (OLAF), and more broadly with European counterparts through Eurofisc.⁷² The GBFI proactively engages with High Tech Crime Forum established by the Banking and Payments Federation of Ireland (BPF) to share intelligence on detected financial crime trends and typologies with industry representatives.

Fraud, deception and related offences accounted for over 2% of all recorded offences in 2015.⁷³ Given the complex nature and under-reporting of financial crime, it is difficult to estimate the full extent and scale of financial crime in Ireland. Estimates suggest that the average cost of fraud to organisations was €1.7 million in 2015, an increase from approximately €500,000 in 2014.⁷⁴ Recoveries of social welfare overpayments amounted to almost €86.3 million in 2014 and €83 million in 2015.⁷⁵

Law enforcement intelligence suggests that the proceeds generated by financial crime, including social welfare fraud and computer enabled financial crime are processed by means of electronic payments, with money often moved quickly through the banking, payments, and financial sectors. There is evidence that mule accounts, bogus accounts, or opaque corporate accounts are used to launder proceeds. An emerging trend is the use of cryptocurrencies, such as Bitcoin, to launder the proceeds of computer-enabled financial crime, i.e. crimes such as phishing frauds committed with the assistance of general (e.g. email) and specialised (e.g. payment services) IT systems. Intelligence suggests that the scale and interconnectedness of Ireland's financial system indicates the proceeds of some foreign financial crimes may pass through the Irish financial system without coming to the attention of Irish credit or financial institutions.

⁷¹ OCP report estimates range from 122 to 215 million euro
<http://www.transcrime.it/wp-content/uploads/2015/12/ocp.pdf>.

⁷² Council of the European Union, Press Release 14349/10, Council strengthens cooperation on VAT fraud and creates Eurofisc network to detect new fraud schemes, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/116920.pdf

⁷³ CSO, Recorded crime incidents classified by offence group and annualised total, Q1 2015 and 2016, <http://www.cso.ie/en/releasesandpublications/er/rc/recordedcrimequarter12016/>

⁷⁴ PwC, 2016 Irish Economic Crime Survey "Economic crime: A rising threat in Ireland", p 10

⁷⁵ Department of Social Protection, Compliance & Anti-Fraud Strategy 2014 – 2018, Annual Report 2015 & Annual Target Statement 2016, April 2016, <http://www.welfare.ie/en/downloads/DSP-Compliance-AntiFraud-Strategy-2014-2018.pdf> p 3

Tobacco Smuggling

Tobacco smuggling represents a significant and increasing threat of money laundering to Ireland due to a number of factors. The excise duty levied on cigarettes and tobacco products is high and amounts to approximately 78% of the retail price of cigarettes.⁷⁶ The higher profitability of illicit tobacco products is attractive to criminals, in particular OCGs. In addition, the effectiveness of law enforcement and technical measures to prevent fuel smuggling may have increased OCG tobacco smuggling.

Tobacco generated over €1 billion in excise duty in 2015⁷⁷ and while it is difficult to estimate the full extent and scale of tobacco smuggling in Ireland, estimates suggest that consumption of illicit tobacco products amounted to 11% of overall consumption in 2013.⁷⁸ Illicit tobacco products valued at over €35 million were seized by Revenue in 2015.⁷⁹

Law enforcement intelligence suggests that the illicit tobacco products, including counterfeit products, entering the Irish market originate primarily from Eastern Europe and Asia. Such products often land in Ireland as the point of entry to the EU or other European markets. Illicit tobacco is often transported in a manner similar to illicit drugs via established international trade routes. Law enforcement authorities have observed a recent trend towards containerised shipment of tobacco products.⁸⁰ Intelligence indicates that OCGs involved in tobacco smuggling are often also involved in drug trafficking. Law enforcement and customs authorities actively collaborate and share intelligence with UK, European and international counterparts to detect and prevent illicit tobacco from entering the EU through Ireland.⁸¹ In 2015, there were 115 convictions for tobacco offences; there were 111 convictions in 2014.⁸²

Due to the nature of illicit tobacco sales, the proceeds generated are largely in cash. Law enforcement intelligence suggests that bulk cash transportation, third party laundering, cash-intensive businesses, money transmission businesses and Bureaux de Change are common methods used by criminals to launder dirty money associated with tobacco smuggling.

Tax Evasion

Public international peer reviews have found that Ireland operates a highly efficient and transparent tax regime which is fully compliant with the Organisation for Economic Co-operation and Development's (OECD) standards.⁸³ Ireland is rated the easiest country in the EU to pay business taxes,⁸⁴ and also the Member State with the second lowest burden of customs procedures in the EU.⁸⁵ Academic research describes Ireland as a small, open economy which displays none of the characteristics of a tax haven.⁸⁶

Ireland is committed to the fight against tax evasion and to reducing tax avoidance. Ireland has a large network of tax treaties with other jurisdictions⁸⁷ and has concluded an intergovernmental Foreign Account Tax Compliance Act (FATCA) agreement with the USA in 2012. Ireland has also introduced legislation to implement the OECD's Common Reporting Standard (CRS) for the automatic exchange of financial information. Ireland is one of the 55 early adopter countries and is due to start exchanging CRS data in 2017. Ireland is actively involved in the OECD Base Erosion and Profit Shifting (BEPS) initiative and has enacted legislation to address BEPS Action 13, on country by country reporting.⁸⁸ This legislation is intended to enhance the transparency of transfer pricing documentation for certain multi-national enterprises. The

⁷⁶ British-Irish Inter-parliamentary Assembly, Report on Cross-border Police Cooperation and Illicit Trade (NI cross-border report), 2015, p 5

⁷⁷ Revenue Commissioners, Annual Report 2015

⁷⁸ NI cross-border report, p 9

⁷⁹ Revenue Commissioners, Annual Report 2015

⁸⁰ E.g. cigarettes valued at €4.5 million seized from MS Cosco Fortune originating from China in May 2015

⁸¹ See <http://www.irishtimes.com/news/crime-and-law/cigarettes-worth-2-1m-seized-by-revenue-on-m-1-1.2417046>; cigarettes valued at €2.4 million seized in Rosslare Europort in September 2014; tobacco products valued at €1.4 million seized in Drogheda Port in June 2014

⁸² Information furnished to the AMLSC by Revenue Commissioners

⁸³ Global Forum Peer Review Report 2011

⁸⁴ PwC & World Bank, Paying Taxes Report 2016

⁸⁵ World Economic Forum, Global Competitiveness Index 2016

⁸⁶ Tobin & Walsh, "What makes a country a tax haven? As assessment of international standards shows why Ireland is not a tax haven" (2013), *The Economic and Social Review*, Vol. 44, No. 3, 401

⁸⁷ 72 Double Taxation Agreements and 25 Tax Information Exchange Agreements

⁸⁸ Finance Act 2015 s(33), Taxes (Country by Country Reporting) Regulations 2015 SI 2015/629

legislation requires certain multi-national enterprises to file a country-by-country report that will provide annually, and for each tax jurisdiction in which they do business, the amount of revenue, profit before income tax and income tax paid and accrued and other indicators of economic activities.

Ireland is a strong supporter of the European Commission's work in the area of tax transparency and administrative cooperation. In addition, Ireland is committed to:

- The full exchange of tax information with tax treaty partners;
- Global automatic exchange of tax information, in line with existing and emerging EU and OECD rules;
- Actively contributing to the OECD and EU efforts to tackle harmful tax competition; and
- Engaging constructively and respectfully with developing countries in relation to tax matters by offering assistance wherever possible.⁸⁹

The detection, investigation and sanctioning of tax offences is undertaken collaboratively between Revenue, SIU, and CAB to leverage the full extent of information available to the authorities and to coordinate action. Revenue receives suspicious transaction reports from financial institutions, and other designated bodies, in parallel with the Financial Intelligence Unit within An Garda Síochána. Ireland is unique in implementing a dual-reporting requirement for STRs. Revenue operates a Financial Intelligence Section to analyse received STRs.

Revenue actively conducts audit and compliance interventions to address tax evasion, tax avoidance, and shadow economy activities across the entire taxpayer base. Revenue is committed to using its extensive powers to identify and address suspected tax evasion and tax avoidance, including the use of offshore assets and accounts. In 2015, Revenue actions in the area of offshore assets and trusts yielded approximately €60 million,⁹⁰ with a further €42 million raised from the settling of tax avoidance cases.⁹¹

In total, Revenue collected taxes and duties in the amount of €45.79 billion in 2015. Revenue raised €642.5 million from audit and compliance interventions in 2015. This amounts to approximately 1.4% of the total collected by Revenue in 2015. In addition, CAB served tax demands in the amount of approximately €11 million and recovered approximately €3 million in 2014.⁹² Revenue secured 28 criminal convictions for serious tax evasion in 2015.⁹³ Tax payment compliance rates are, however, generally high,⁹⁴ with only a small minority of taxpayers choosing not to comply with their tax and duty obligations.⁹⁵

Prostitution

Prostitution in Ireland is often linked to human trafficking and organised and conducted by OCGs. Law enforcement intelligence suggests that people are trafficked into Ireland for sexual exploitation. As such, both foreign and domestic OCGs are known to be involved in prostitution in Ireland with many of those OCGs also involved in other illicit activities such as drug smuggling, alcohol or fuel smuggling.

While Irish law does not criminalise the purchase or sale of sexual services, activities associated with prostitution such as pimping, soliciting or brothel keeping are crimes. It is also an offence to organise prostitution, coerce or compel a person to be a prostitute or to knowingly live off the earnings of a prostitute. The Criminal Justice (Sexual Offences) Bill 2015, when enacted, will criminalise the purchase of sexual services. There were 56 recorded prostitution offences in 2015. This compares with 129 in 2014 and 120 in 2013.⁹⁶

⁸⁹ Department of Finance, Update on Ireland's International Tax Strategy, October 2015

⁹⁰ Revenue Commissioners, Annual Report 2015, p 29

⁹¹ *Ibid* p 9

⁹² Criminal Assets Bureau, Annual Report 2014, p 22

⁹³ Revenue Commissioners, Annual Report 2015, p 10

⁹⁴ *Ibid* p 77

⁹⁵ *Ibid* p 9

⁹⁶ CSO, Recorded Crime Offences (Number) by Type of Offence and Year, <http://www.cso.ie/multiquicktables/quickTables.aspx?id=cja01>

Law enforcement authorities conduct a range of targeted operations against prostitution and brothel-keeping OCGs to disrupt and prevent their operation. Law enforcement authorities are committed to enhancing inter-agency cooperation to improve the detection, investigation and prosecution of prostitution offences. An Garda Síochána continues to cooperate with Non-Government Organisations, developing joint training programmes and seminars highlighting the complexities associated with prostitution investigations. These training programmes and seminars are delivered to both members of An Garda Síochána and other European law enforcement agencies. In addition An Garda Síochána cooperate with European and International law enforcement agencies such as Europol, Interpol and other national police forces in the investigation of prostitution offences.

There are intelligence gaps in respect of the full extent and scale of prostitution in Ireland. However, prostitution is known to involve hundreds of people in Ireland and Garda investigations have revealed the involvement of a significant number of OCGs. Prostitution is known to generate substantial sums of money, typically in cash. Law enforcement intelligence suggests that criminals involved in prostitution move significant sums of money out of Ireland using cash mules. OCGs are also known to use extended family networks to launder cash. In addition, law enforcement intelligence suggests that cash-intensive businesses, money remittance firms and third party cash lodgements into bank accounts are also common methods for laundering the proceeds of prostitution.

Fuel Laundering

Fuel laundering involves the illegal removal of marker dyes from cheaper,⁹⁷ non-road fuels and reselling the laundered fuel to customers, at a significant profit. Fuel laundering is known to be a source of funds for OCGs in Ireland. Fuel laundering has been known to be prevalent in areas close to the border where criminals may attempt to take advantage of the cross-border currency, tax and pricing differences between Ireland and the UK.⁹⁸ As such, it has the potential to generate significant levels of proceeds.

The detection and prevention of fuel laundering is a key priority for law enforcement authorities and both Revenue and CAB have committed significant resources to these activities. Revenue and CAB undertake robust and sustained enforcement actions against perpetrators of fuel laundering, at all stages of the supply chain, in an attempt to prevent fuel reaching the market. Since mid-2011, 134 filling stations have been closed for breaches of licensing conditions, over 3 million litres of fuel have been seized and 31 oil laundries detected and closed down.⁹⁹

In addition, close cross-border collaboration between Irish and UK law enforcement authorities has contributed to a significant decrease in laundered fuel. This has been supported by a joint initiative between Revenue and Her Majesty's Revenue and Customs (HMRC) to find a more effective marker dye for non-road fuels, together with an intensified fuel testing programme, compliance project and enforcement actions during 2015. By the end of 2015, over 500 premises were visited by Revenue with 1000 samples tested. In addition, a cross-border multi-agency taskforce, The Cross-Border Fuel Fraud Enforcement Group, has been established to combat fuel laundering on an all-island basis.¹⁰⁰

In addition, feedback from traders and representative bodies has confirmed a significant reduction in fuel laundering since the new initiatives were introduced.¹⁰¹ While this is welcome news, law enforcement authorities remain committed to combatting fuel laundering on an all-island basis and to monitoring emerging trends.

It is difficult to estimate the full extent and scale of fuel laundering and the associated tax loss to the exchequer. However, Revenue estimates that its enhanced activities combatting fuel laundering contributed approximately €200 million in taxes and duties to the exchequer in 2014.¹⁰² In 2015 approximately

⁹⁷ See Department of Finance, TSG14/03, <http://www.finance.gov.ie/sites/default/files/14.03%20Energy%20%20Environmental%20Taxes.pdf>

⁹⁸ Revenue Commissioners, Cross-Border Price Comparisons July 2015

⁹⁹ Information provided by Revenue

¹⁰⁰ Revenue Commissioners, Annual Report 2015, p 33

¹⁰¹ *Ibid*

¹⁰² *Ibid*

215,000 litres of fuel was seized with 310 summary convictions.¹⁰³ In addition, targeted audit interventions yielded €2.7 million in tax, interest and penalties over 76 audits.¹⁰⁴

Sample testing, conducted in early 2016, under the independent supervision of Revenue's Statistics and Economics Research Branch, shows that the selling of laundered fuel in the market is now negligible and close to being fully eliminated.¹⁰⁵

Law enforcement intelligence confirms that the proceeds generated as a result of fuel laundering are largely in cash. Criminals launder these proceeds using a number of means including:

- Establishing or becoming involved in cash intensive businesses such as high value goods dealers (HVGDs), wholesale businesses, transportation businesses, filling stations;
- Trade based money laundering, which is the movement of goods through the trade system;
- Bureau de Change;
- Money transmission businesses;
- Cash mules; and
- Third party money laundering.

Theft and Burglary

Theft and burglary in Ireland is perpetrated by a wide range of individuals, domestic OCGs and foreign OCGs. Theft offences range in scale and sophistication from opportunistic theft to organised and systematic theft, such as metal, vehicle and plant and machinery theft. Intelligence confirms that these organised thefts generate significant proceeds and are largely perpetrated by domestic and foreign OCGs.

Theft and burglary related offences are the most commonly recorded offences in Ireland. There were over 100,000 recorded theft and burglary related offences recorded in 2015, amounting to almost 45% of all recorded offences.¹⁰⁶ Despite the high numbers of offences recorded, intelligence confirms that the majority of theft offences are smaller scale thefts where stolen property is often recovered before it can be laundered.

Due to the wide range of theft offences, underreporting of theft and difficulty in quantifying the value of stolen property, it is difficult to estimate the full scale of proceeds generated. However, it is known that theft generates significant proceeds of crime.

Metal Theft

Metal theft is an increasingly common phenomenon in Ireland. The rising demand for metals on the international market and rising commodity prices increases the proceeds that can be generated from metal theft. It is known that foreign OCGs are involved in sophisticated metal thefts affecting the transport, utility, recycling and communications sectors.

Vehicle Theft

Despite having one of the lower overall theft rates for vehicles in the EU and one of the highest recovery rates, vehicle theft remains a significant source of proceeds for OCGs. Approximately 7,800 vehicles were stolen in 2014 and 68% of those were subsequently recovered.¹⁰⁷

Both domestic and foreign OCGs are involved in organised vehicle theft. It is known that a significant proportion of vehicles can be stolen to order, either for the use in the commission of a further offence, or

¹⁰³ *Ibid* p 79 - 80

¹⁰⁴ *Ibid* p 9

¹⁰⁵ Information furnished to the AMLSC by Revenue Commissioners

¹⁰⁶ CSO, CJA01: Recorded Crime Offences by Type of Offence and Year,

<http://www.cso.ie/px/pxeirestat/statire/SelectVarVal/Define.asp?Maintable=CJA01&PLanguage=0>

¹⁰⁷ Information furnished to the AMLSC by An Garda Síochána

to be exported. A significant proportion of vehicles are stolen to be subsequently dismantled into parts for sale or for exportation out of Ireland.

An emerging trend is the theft of high end vehicles. Criminals are using sophisticated electronic systems to defeat the “keyless entry” systems used on the majority of these vehicles. Intelligence suggests that the majority of these thefts are for export to Eastern Europe or to Asia.

While the replacement value for stolen vehicles is high, intelligence suggests that the black market value of vehicles is significantly lower.

Intelligence suggests that the proceeds of vehicle theft are largely in cash and are laundered through businesses, such as HVGDs or other cash intensive businesses, or used by OCGs to fund further drug trafficking activities.

Plant and Machinery Theft

Due to the downturn in construction activity in Ireland in recent years, there has been a decrease in demand for plant and machinery across the country and there has also been a decrease in the number of assets present in the country. Intelligence suggests that most plant and machinery assets were exported to emerging markets as domestic demand declined. This, together with an increase in detection and prevention activities by An Garda Síochána,¹⁰⁸ and the “Theft Stop” joint initiative with the Irish Farmers Association, has contributed to an overall decline. There have been recent increases in the recovery rates for some asset types. Due to intelligence gaps, it is difficult to estimate the full scale of plant and machinery theft in Ireland.

In comparison to vehicle theft, the theft of plant and machinery typically requires less sophisticated tools and equipment. Intelligence suggests that perpetrators commonly use businesses to enable the sale or export of stolen plant and machinery. In addition, intelligence suggests that a proportion of stolen agricultural machinery is sold via online marketplaces. Perpetrators may also engage in financing or insurance fraud, in relation to plant and machinery.

Intelligence confirms that OCGs are the main perpetrators of plant and machinery theft, and that the proceeds of plant and machinery theft are typically laundered through businesses such as HVGDs or other cash intensive businesses, or used by OCGs to fund further criminal activities.

Cybercrime

Cybercrime refers to a wide range of criminal activities which involve computers and information systems as tools, targets or enablers. Examples of such offences are: malware; denial of service attacks, hacking, intellectual property theft and industrial espionage, cyber extortion, and software counterfeiting.

Research suggests that 44% of Irish businesses are impacted by cybercrime,¹⁰⁹ which is almost double the rate in 2012, and that 36% of Irish businesses view cybercrime as the greatest future risk.¹¹⁰ The money laundering impact of cybercrime can arise from the direct exploitation of stolen resources, e.g. fraudulent use of a credit card, or the sale of stolen resources, e.g. sale of intellectual property.

Cybercrime can be perpetrated by company insiders, domestic and foreign OCGs, malicious hackers, or terrorist organisations. It is also known that cybercrime is perpetrated against individuals, businesses and government entities.

Law enforcement intelligence suggests that the proceeds of cybercrime are typically electronic payments which are transferred through the financial system, money remittance firms and, more recently, using cryptocurrencies such as Bitcoin. The use of cryptocurrencies is common in Distributed Denial of Service (DDoS) attacks and malware/ransomware attacks. Criminals use money mule accounts to launder the proceeds of cybercrime committed in Ireland and abroad. Cybercrime is an emerging and fast-developing category of criminal activity affecting Ireland.

¹⁰⁸ Operations Segund, Skipper and Mocha

¹⁰⁹ PwC, p 8

¹¹⁰ *Ibid* p 12

Human Trafficking

Human trafficking in Ireland is organised and conducted by OCGs and, as noted above, it is closely related to OCG prostitution activity. Intelligence¹¹¹ suggests that significant numbers of people are trafficked into Ireland for sexual exploitation from a range of countries across Africa, Eastern Europe, and Asia,¹¹² and from directly across Ireland's border with the UK.

Intelligence suggests that victims may be forced to commit a range of offences including:

- Sexual exploitation,
- Labour exploitation,
- Forced criminal activities involving gain.

Due to the cross-border nature of human trafficking, there are intelligence gaps in respect of the nature and scale of human trafficking in Ireland, the nature of the proceeds and how the proceeds are laundered. However, evidence suggests that human trafficking is a growing threat to Ireland and that the majority of proceeds generated are in cash.

Intelligence suggests that OCGs often rely on extended family networks to enable the distribution and laundering of cash. Cash mules, cash-intensive businesses, money remittance firms and third party cash lodgements into bank accounts are also common methods for laundering the proceeds of human trafficking. Due to the exploitative nature of human trafficking, perpetrators often control victims' identification documents and open bank accounts on victims' behalf to use for money laundering purposes.

An Garda Síochána continues to cooperate with Non-Government Organisations (NGOs) to enhance measures to combat human trafficking. In addition, An Garda Síochána cooperates with European and International law enforcement agencies such as Europol, Interpol and other national police forces, in the investigation and combatting of human trafficking. An Garda Síochána adopts a multi-disciplinary approach to the investigation of human trafficking to provide a holistic and victim-centric solution to combatting both human trafficking and prostitution. The objective of An Garda Síochána's strategy is consistent with the Human Trafficking National Action Plan's priorities: Prevention; Protection; Prosecution and Partnership.

Bribery and Corruption

Perpetrators of bribery and corruption offences can include private individuals, corporate entities and public officials. Perpetrators include the giver and receiver of the monies or favour. Perpetrators of corruption are generally sophisticated and adept at avoiding detection. In addition, perpetrators can include Irish citizens bribing or attempting to bribe foreign public officials to achieve business objectives, particularly in emerging markets.

Bribery and corruption are global phenomena to which Ireland is not immune. However, Ireland is among the 20 least corrupt countries in the world according to the "Transparency International Corruption Perception Index" for 2015.

Ireland remains committed to combatting bribery and corruption at home and abroad, in order to maintain a transparent and corruption free environment. The United Nations Office on Drugs and Crime (UNODC), in reviewing Ireland's implementation of the Convention against Corruption, recognises the successes and good practices currently in place. Examples of these are in the areas of whistleblower protection, the broad scope of current legislation, the non-conviction based confiscation measures,¹¹³ the role of the

¹¹¹ Department of Justice and Equality, Second National Action Plan to Prevent and Combat Human Trafficking in Ireland 2015, p 20 ('Action Plan')

¹¹² OCP, p 108

¹¹³ Proceeds of Crime Act 1996; Criminal Assets Bureau Act 1996; Criminal Justice Act 1994; Prevention of Corruption (Amendment) Act 2001

Criminal Assets Bureau and the non-existence of immunities from prosecution for public officials other than the President.¹¹⁴

Ireland has introduced significant improvements in the areas of whistleblower protection¹¹⁵ and the regulation and transparency of public sector lobbying.¹¹⁶ In addition, the Government is committed to enacting the Criminal Justice (Corruption) Bill which will replace the existing legislative framework, the Prevention of Corruption Acts up to 2010. The Bill will consolidate and strengthen Ireland's anti-corruption legislation and will include measures such as:

- Expanding the range of offences and penalties applicable;
- A presumption of corruption in respect of corrupt enrichment of public officials;
- Introduction of corporate liability; and
- Expansion of the extraterritorial effect of anti-corruption legislation.

While intelligence suggests that the incidence of bribery and corruption is low in Ireland, it is difficult to estimate the full extent of occurrence of such offences and the scale of proceeds involved. However, it is not believed to be a significant money laundering threat in Ireland. This difficulty is increased in the case of foreign bribery in particular, where investigations and prosecutions can be difficult to pursue due to law enforcement intelligence, capability, and resourcing gaps. However, intelligence suggests that cash payments are most common for domestic bribery and that electronic payments are most common for foreign bribery.

Other Illicit Trade

Counterfeiting, intellectual property theft, and other forms of illicit trade are emerging threats of money laundering in Ireland. Criminals exploit consumer demand for high value products, and products subject to high levels of excise duty, to generate significant levels of profit. Despite intelligence gaps, evidence suggests that illicit trade generates significant proceeds of crime and is a significant money laundering threat.

Law enforcement intelligence suggests that perpetrators can include a wide range of criminals including domestic and foreign OCGs, opportunist criminals and individuals. It is known that OCGs involved in illicit trade, such as counterfeiting and intellectual property theft, operate as part of international criminal networks with links to the other OCGs and suppliers in the Middle East and Asia. Counterfeit products are imported into Ireland through established, legitimate, trade routes with consignments often disguised as legitimate products to conceal their nature.

Due to intelligence gaps, it is difficult to estimate the scale of the proceeds generated by these criminal activities. Intelligence suggests that the emergence and growth of online advertising and purchasing has increased the availability of illicit products in Ireland. This has resulted in an increase in the overall scale of criminal activity in this area. As such, perpetrators can use a wide range of methods and means to launder the proceeds of illicit trade. These methods vary according to the nature of the perpetrator and illicit activity involved but can include:

- Money remittance firms;
- Bureau de Change;
- Banks;
- Cash mules; and
- Cryptocurrencies.

¹¹⁴ United Nations Office on Drugs and Crime, Country Review Report of Ireland 2015, p 7

¹¹⁵ Protected Disclosures Act 2014

¹¹⁶ Regulation of Lobbying Act 2015

Alcohol

Alcohol smugglers and counterfeiters may exploit the price and tax differentials between Ireland and other European countries.

OCGs are known perpetrators of alcohol smuggling and counterfeiting. Intelligence suggests that these OCGs are often connected with foreign OCGs to enable the sourcing or production of illicit alcohol products. It is known that there is significant illicit alcohol activity in areas close to Ireland's border with the UK.¹¹⁷

There was a significant increase in illicit alcohol seizures in 2015 with 938 seizures¹¹⁸ compared to 550 in 2014 and 507 in 2013. These seizures were valued at approximately €600,000 in 2015 and 2014 and approximately €1,500,000 in 2013. Despite the increasing number of seizures, reported convictions have remained low in recent years with 5 convictions reported in 2015, 9 convictions reported in 2014 and 7 convictions reported in 2013.¹¹⁹

An internal review by the Revenue Commissioners of Alcohol Products Tax Regime was completed in March 2015. The incidence and experience of alcohol fraud formed part of this review and evidence of large scale alcohol fraud or EMCS fraud (Excise Movement Control System for duty suspended product) resulting in losses to the Irish Exchequer, was not found by this review.

The high level of EMCS diversion fraud experienced in recent years by the UK and Italy indicates that European fraudsters are competent and experienced in EMCS alcohol diversion fraud. While it is recognised that large scale EMCS diversion fraud has not yet been detected in Ireland, it is however considered to pose a significant potential risk in light of the strong financial incentives to evade alcohol tax in Ireland, and the experience of the UK and Italy. To address this risk, Revenue have committed to further develop analytical capability to identify potential frauds on EMCS.

Conclusion

This section described key generators of illicit proceeds and measures taken by law enforcement authorities to address those threats; the following sections examine vulnerabilities, i.e. sectors and activities which may be used by money launderers or financiers of terrorism to facilitate their activities.

¹¹⁷ Police Service of Northern Ireland and An Garda Síochána, Cross Border Organised Crime Assessment 2014

¹¹⁸ Revenue Commissioners, Annual Report 2015, p 79

¹¹⁹ Revenue Commissioners, Annual Reports 2013 - 2015

Financial Services Sector

6

Financial Services Sector

The financial services sector is a significant contributor to the Irish economy. The sector plays an important role in Ireland's export-orientated economy, with over 35,000 people directly employed by over 400 international financial services companies,¹²⁰ and contributing 8% of Ireland's GDP in 2014.¹²¹ Ireland is the 4th largest exporter of Financial Services in the EU.¹²²

The Central Bank of Ireland is the competent authority for AML/CFT supervision for the credit and financial institutions in Ireland under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended. The Central Bank has a dual mandate as a central bank and a financial regulator. In its role as financial regulator it is responsible for the licensing, prudential and consumer protection supervision and enforcement of regulatory requirements. The Central Bank became competent authority for AML/CFT supervision in July 2010.

The Central Bank adopts a risk-sensitive approach to AML/CFT supervision and maintains a ML/TF risk assessment to ensure its AML/CFT supervisory approach is based on ML/TF risk.

The Central Bank is responsible for monitoring credit and financial institutions' compliance with AML/CFT obligations and it takes necessary measures to ensure compliance, which include remedial actions and referring cases for enforcement action to be taken, if appropriate. The Central Bank actively promotes an awareness of AML/CFT obligations and ML/TF risks to the financial services sector.

This section sets out Ireland's understanding of the ML/TF risks present in the sub-sectors within the Irish Financial Services Sector. This assessment draws on the knowledge, experience and professional judgment of Ireland's competent authorities and law enforcement agencies to assess the known threats and vulnerabilities relevant to the Financial Services Sector. In addition, statistical information relating to Suspicious Transaction Reports from the FIU and the Revenue Commissioners was considered in the course of the assessment. Factors considered during the assessment include:

- the nature and scale of the ML/TF threats;
- the nature, scale and complexity of the sectors;
- the types of customers relevant to the sectors;
- the distribution channels typically used;
- the products and services offered in the sectors; and
- mitigants and any other relevant factors.

¹²⁰ Department of Finance, IFS2020: A Strategy for Ireland's International Financial Services Sector 2015-2020, March 2015, <http://www.finance.gov.ie/sites/default/files/IFS2020.pdf>

¹²¹ CSO, Institutional Sector Accounts Non-Financial and Financial 2014, <http://www.cso.ie/en/releasesandpublications/ep/p-isanff/isanff2014/summarytable/>

¹²² *Ibid*

Overview of ML and TF Risks in Financial Services Sector

The financial services sector as a whole is at risk of being targeted by criminals to launder the proceeds of crime and finance terrorism due to a range of factors, including:

- the wide range of products and services offered in the sector;
- the nature of the products and services offered;
- the broad demographic of the customer base;
- the wide geographic reach of the financial sector;
- the scale and materiality of the financial sector in Ireland;
- the use of complex corporate vehicles.

Individual sectors within the broader financial services sector are considered in detail below.

The financial services sector as a whole is vulnerable to ML/TF threats arising from a range of predicate offences including drug trafficking, financial crime, fuel smuggling, prostitution, tax evasion, bribery and corruption. These are set out in greater detail in Chapter 5.

Retail Banking

Overview

Retail banking is central to the Irish financial system. The sector is highly concentrated, comprising 5 core retail banks as at 30 April 2016. Retail banks play an important role as gatekeeper to the financial system as businesses must usually engage their services which are essential to operations such as paying employees and vendors or financing capital expenditure. The banks provide a full range of general banking services to both individuals and businesses, which include; current and savings accounts, loan and investment products, and payment transmission services. A number of these banks also offer wholesale banking products and services such as correspondent banking and trade financing.

Retail banks have an inclusion rate of circa 80% of the adult population,¹²³ with most of these customers requiring a bank account to pay bills, receive salaries and conduct business. The majority of retail banking customers are domestic customers with many having a long relationship with the same bank. They also offer a wide variety of products and services including facilities to non-residents.

Irish retail banks operate primarily through an extensive countrywide branch network, with multiple banks offering branch facilities in the same locality. In addition to the branch network, retail banks provide services to customers via the internet, mobile applications, post and telephone.

Retail banks process high volumes of transactions on a daily basis. These transactions are conducted through a range of channels, including online and in branch with indications that online transaction volumes as a percentage of overall transactions are significant and growing.

Electronic payments enable the rapid movement of funds between accounts both domestically and internationally. A large volume of transactions are also processed through the network of 3,065 ATMs provided by retail banks countrywide, with 163.1 million ATM withdrawals at a value of €20.3 million processed in 2014.¹²⁴

Main Vulnerabilities

The nature, scale and complexity of Irish retail banks make them vulnerable to all stages of the ML process and vulnerable to TF due to their central function within the financial system. While the likelihood of a specific customer or transaction being used for ML or TF is low, the volume of both poses a key challenge to banks in terms of monitoring and identifying suspicious activity. In particular, the number of international

¹²³ National Payments Plan 2013, <https://www.centralbank.ie/paycurr/paysys/Documents/National%20Payments%20Plan%20-%20Final%20Version.pdf>

¹²⁴ BPI Annual Payment Statistics, <http://www.bpfi.ie/wp-content/uploads/2015/05/BPFI-Payment-Statistics-2014-Data-Report.pdf>

transactions creates opportunities for misuse especially where the origin or path of funds is not fully disclosed. The potential ML/TF risk associated with such international transactions increases when funds are transmitted to or from jurisdictions outside EEA, which may have inadequate AML regulation and controls.

Retail banks offer a wide range of products and services with features that increase the ML/TF risk. Such features include:

- cash-intensive nature of some products;
- online transaction capabilities;
- electronic payments to non-equivalent jurisdictions;
- access to banking services by third parties, for example lodgements to third party accounts and credit cards; and
- Bureau de Change services which can also be availed of by non-bank customers, subject to certain thresholds.

The wide reach of retail banks' customer base leaves the sector vulnerable to ML or TF. The customer base includes customers who may be sought out by criminals to facilitate the laundering of illicit funds. These include:

- cash-intensive businesses, e.g. retailers, petrol stations, bookmakers;
- charities and not for profit organisations;
- lawyers, accountants and other professionals;
- Politically Exposed Persons;
- high net worth individuals; and
- complex corporate structures.

ML/TF risk is also increased through the ease of moving funds which private and corporate banking facilities may afford.

The reduction in the level of face-to-face interaction between retail banks and their customers due to the emergence and evolution of online banking poses a challenge to banks knowing their customers and increases the importance of adequate CDD and transaction monitoring in retail banks.

In terms of geographical risk, particular concerns arise in relation to the border (e.g. in relation to the use of banking to launder the proceeds of certain predicate offences such as fuel laundering and tobacco smuggling).

Overall Risk

The overall ML/TF risk within the Irish retail banking sector is judged to be **High**, due to the nature, scale and complexity of the sector and its central role in Irish financial services, offering core banking services to a broad population and acting as the gateway to the wider financial sector. In addition, STR statistics for 2015 indicated that 62% of all STRs reported in 2015 were raised by credit institutions;ⁱ it is understood that the majority of STRs raised were reported by the core retail banks.

Non-Retail Banks

Overview

As at 30 April 2016, the non-retail banking sector encompassed 17 credit institutions authorised and operating in Ireland, in addition to a further 29 branches of European credit institutions operating in Ireland on a freedom of establishment basis. These institutions are sometimes known as wholesale banks.

Non-retail banks have a significant presence in the Irish financial services sector and many of these firms are global entities with parents or subsidiaries in Europe or the United States of America. Ireland has been identified as being the location for the second highest amount of assets located in foreign controlled banking group subsidiaries and branches in 2013, with €514 billion euros of assets.¹²⁵

The non-retail banking sector is complex and offers a broad range of products and services to a wide variety of individual and business customers. Such products and services include:

- correspondent banking;
- trade finance;
- syndicated lending; and
- wealth management.

Customers of non-retail banks are both domestic and international in origin and generally operate at the 'high end' of the market. Customers typically include:

- professional clients;
- high net worth individuals;
- trusts;
- partnerships;
- charities;
- corporates; and
- regulated designated persons (such as banks, investment firms, and funds).

Main Vulnerabilities

The nature, scale, complexity and interconnectedness of the non-retail banking sector make it vulnerable to ML/TF. This is reinforced by the high level of assets of Irish non-retail banks and the high transaction values and volumes.

The geographically diverse customer base exposes the sector to a higher proportion of customers who would be classified as "high risk" such as:

- PEPs;
- complex cross-jurisdictional ownership structures; or
- potentially sanctioned individuals.

This sector offers a wide range of products and services (as mentioned above) which have features that have potential to increase the ML/TF risk.

The delivery channels used by non-retail banks to deliver their products and services to customers are equally diverse. Much of the business undertaken is non-face to face, with a high proportion of business conducted indirectly through intermediaries, and can also involve large scale online transactions and electronic payments. Customer numbers, transaction volumes and values are high and can often be complex and cross jurisdictional; often outside the EEA and involving high risk jurisdictions, which can create difficulties in tracking ownership and the flow of funds.

¹²⁵ Statista, Assets of foreign controlled banking group subs & branches 2013, <http://www.statista.com/statistics/354224/eu18-foreign-controlled-banks-assets/>

The combination of the above factors, and in particular the broad demographic of clients and geographical transactional reach of this sector expose it to a higher risk of ML/TF.

However, while some non-retail banks provide higher risk products and services, other non-retail banks provide lower risk products and services. Such firms include covered banks whose main purpose is to raise funds for their parent institution.

Overall Risk

The ML/TF risk for the non-retail banking sector is assessed as **Medium High**. Non-retail banks have a global presence and jurisdictional reach in terms of customers, products and transactions. This exposes the sector to high risk jurisdictions from an ML/TF perspective. The majority of business conducted by non-retail banks is non-face to face with the use of electronic commerce to complete transactions. This increases the ML/TF risk due to the ease of access and speed to which transactions may be completed, potential for anonymity and use by third parties. The products and services offered by many non-retail banks are diverse and complex. The use of complex products may make it difficult to identify the ultimate beneficial owner and the source of funds, thus increasing the ML risk. Notwithstanding this, certain non-retail banks provide lower risk services to lower risk customers, for example raising funds for their parent entity, which brings the overall risk rating of the sector to medium high.

Payment Institutions

As at 30 April 2016, there were 12 payment institutions (PIs) authorised by the Central Bank. Overall risk for payment institutions is largely driven by the nature of the services being provided. As a result, this section will split the PI sector into two broad types in order to properly distinguish between them:

1. PIs who offer conventional money remittance services only and agents of same;
2. Other payment institutions which do not provide cash-based money remittance services.

Money Remittance Firms

Overview

Services provided by money remittance firms serve as an alternative value transfer system in lieu of services offered by traditional credit institutions and, in addition, those services often have a wider geographical reach and penetration than similar services offered by credit institutions.

Main Vulnerabilities

The high-volume, cash-based nature of transactions is a significant vulnerability for money remitters, which is usually low-value in nature. Services are provided to customers on a purely transactional basis and as such, a business relationship is not formed with the customer. The relationship between the money remitter and the customer is transient in nature. As transaction values typically fall under CDD thresholds, there is a risk that PEPs and other high risk customers will not be identified.

The use of agents is a common feature of the money remittance business model. Many such agents are often not otherwise in the financial services industry and offer such money remittance services as an ancillary activity to their main business. For example, retailers, grocery shops, salons and other small businesses may offer money remittance services at the point of sale. The extent and variety of operators within a remitter's agency network can pose challenges for the remitter in maintaining adequate oversight of their agents, to ensure that they are complying with their legal and regulatory requirements.

Many EEA money remitters utilising their "European Passport" have also established extensive networks of Irish agents and branches. Such EEA firms come under the Central Bank's AML/CFT supervisory remit in respect of their Irish branches and/ or agency networks. As at 30 April 2016, there were 21 branches of EEA money remitters established in Ireland.

The majority of money remittance business involves funds being transferred from Ireland to foreign jurisdictions and the Central Bank of Ireland understands that a sizable proportion of such remittances are to jurisdictions outside the EU. The most significant outflows follow the major migrant routes into Ireland.

Overall Risk

The nature of the service provided exposes money remitters to **High** ML/TF risk because of the easily accessible nature of the service and because of the wide jurisdictional reach of money remittance services. Money remitters deal with high volumes of low value and instant transactions, which are predominantly cash based. In addition, money remitters tend to facilitate once off transactions as opposed to providing services to an established existing customer base. Money remitters may use extensive networks of agents to provide payment services on their behalf. The services provided by these agents are often ancillary to an agent's core business, which is not related to financial services e.g. newsagents. Statistics for 2015 indicated that over 6% of all STRs reported in 2015 were raised by payment institutions.¹²⁶

Payment Institutions other than Money Remitters

Overview

The remaining payment institutions authorised by the Central Bank, offer a diverse range of services, including the processing of electronic transactions. There is a strong ecosystem of payment services companies based and operating in Ireland, providing products and services to a broad and diverse customer base, from individuals to large corporate customers. Such products and services include:

- Merchant acquirer services;
- Currency exchange services;
- Payment account services;
- SEPA credit transfer services; and
- Debt management related services.

Main Vulnerabilities

The non-face to face delivery of products and services to customers in the sector, including emerging innovations in online and mobile transaction technologies, the high transaction volumes, and broad geographic reach for some firms, including some in the merchant acquirer space, increases the vulnerability of this sector to ML/TF.

However, the nature of the products and services being provided, the longevity of customer relationship, the absence of intermediaries in customer relationships, the low transaction values, and the non-cash nature of transactions reduce the risk of money laundering.

Firms which offer services connected to payment accounts can pose a higher ML/TF risk, as typically such services allow customers to place, withdraw, and transfer funds through the payment account using mobile platform technologies. However, in the current Irish context, such risk is limited because customers can only interact with other customers of the particular firm and all monies transfer in or out of payment accounts via the customer's bank account with a regulated credit institution.

Overall Risk

The ML/TF risk rating of the Payment Institutions (other than Money Remitters) sector is assessed as **Medium Low**. While certain payment institutions have high volumes of low value transactions, the nature of the services being provided is lower risk and transactions are not cash based. Delivery of service is predominantly non-face to face and the customer profile can range from natural persons to corporate entities, however the associated risks are reduced by the longevity of customer relationships.

¹²⁶ Financial Intelligence Unit, An Garda Síochána

Bureau de Change

Overview

Bureaux de Change (BdC) are diverse in terms of nature, scale and complexity with a certain number of large domestic and international firms operating in the Irish market. However, the majority of BdCs in Ireland are small, owner-operated businesses, which offer a limited range of products and services. BdCs represent a small part of the overall Irish financial services sector.

Main Vulnerabilities

The cash intensive nature of the products and services offered by BdCs increases the vulnerability of BdCs to ML/TF. The cash intensive nature of the business can facilitate the placement of cash by criminals. It is an attractive mechanism for leaving a low ML/TF audit trail, presenting challenges with regard to the identification of the source of funds, and providing a means to conceal identities and purchasing patterns.

Some BdC owners operate other businesses alongside the primary BdC business, for example money remittance and casino businesses. The cash intensive nature of the combined business heightens the risk that illicit funds may be channelled through the business by criminals. Money remittance services pose an increased ML/TF risk, given their global reach and the ability to move cash rapidly across borders.

BdC customers are predominantly individuals, including tourists, while a minority are corporate entities such as other BdC firms, hotels and traders. Transactions are typically separate, once-off, and infrequent in nature where no business relationship is formed and as a result there is no statutory requirement to obtain CDD when the services are provided, although certain BdC set lower CDD collection thresholds than the statutory threshold in this regard. As such, BdCs face challenges in detecting linked transactions to ascertain if the occasional transaction value threshold of €15,000 has been reached. The majority of transactions are below the threshold set out in Irish legislation. These factors increase the risk of money laundering in BdCs.

The geographic concentration of BdCs in areas close to Ireland's border with the United Kingdom increases the risk of cross-border money laundering or terrorist financing by organised criminal groups for the reasons above.

In some cases, the provision of BdC services is through an agent network. This can increase complexity and make it more challenging for a BdC to oversee regulatory compliance by the agents in turn. However a number of BdC use a Credit Union agent network which reduces the risk associated with those BdCs as Credit Unions are designated persons in their own right.

Overall Risk

BdCs are rated as **High** ML/TF risk because the products and services offered by BdC are cash based, which can present challenges in tracing the origin of funds. Transactions conducted are typically once off in nature and no business relationship is formed. This facilitates customer anonymity as there is no obligation to provide CDD below the statutory occasional value threshold of €15,000, although certain BdC set lower CDD collection thresholds than the statutory threshold. This is a very small sector in Ireland with only 16 BdC authorised as at 30 April 2016. Statistics for 2015 indicated that less than 1% of all STRs reported were raised by Bureau de Change.¹²⁷

¹²⁷ Financial Intelligence Unit, An Garda Síochána

Life Assurance

The insurance sector in Ireland has both domestic and international firms undertaking a variety of business. The sector includes life, non-life, captive, reinsurance and intermediary activities. Intermediary activities are captured separately. This section considers life companies as non-life, captive and reinsurance companies are not designated persons under the Criminal Justice Act 2010.

As of 30 April 2016 there were 47 life companies authorised by the Central Bank. In addition there are 11 life companies that have an Irish branch under the EEA Freedom of Establishment passport and their head office is in another EEA Member State. According to Central Bank of Ireland's 2014 Insurance Statistical Review¹²⁸ almost €32bn of Gross Premium Income was written during 2014.

Life products are generally categorised under the following headings: Protection, Pensions, Savings and Investment. Generally 'protection only' products are regarded as having **low** ML/TF risk as they only pay out on death, disability or serious illness and do not acquire a surrender value. Pensions are also regarded as being **low** risk products as funds are inaccessible for a significant length of time and only payable on retirement. Savings and investment type products, such as single premium policies, policies which have a high cash surrender value or can be used as collateral for loans may be more attractive to potential money launderers or terrorist financiers and are higher risk than protection or pension policies.

This section will discuss the life insurance sector under the following headings:

1. **Domestic Life Insurance** - Life companies writing business in the Irish domestic market;¹²⁹
2. **Cross Border Life Insurance** - Life companies with a head office in Ireland writing business in other EEA Member States under the 'Freedom of Services' or 'Freedom of Establishment's passport regimes and/or writing business outside of the EEA under local rules.

Domestic Life Insurance

Overview

According to the Central Bank of Ireland's 2014 Insurance Statistical Review, €6.6bn of Gross Premium Income was written in the Irish domestic market in 2014. Customers of domestic life companies are mostly natural persons but there are also business customers including limited companies, partnerships, as well as more complex entity structures.

Main Vulnerabilities

Domestic life companies often distribute their products through retail intermediaries and banks. This increases the ML/TF risk in circumstances where the life company relies on the third party for collection of customer due diligence documentation and information. The risk in this regard is mitigated by the fact that distributors of life insurance products must themselves be designated persons under Irish legislation.

Cross Border Life Insurance

Overview

According to the Central Bank's 2014 Insurance Statistical Review, Irish life companies wrote €25bn of Gross Premium Income outside Ireland during that year. Many of the products offered by this sector, do not offer sufficient flexibility to be attractive to money launderers or terrorist financiers for example, protection only or pension products. However much of the €25bn gross premium income arose from single premium investment products which are deemed to be **higher risk**.

Main Vulnerabilities

Irish life companies that write business cross border generally use intermediaries, either banks or retail intermediaries, to distribute their products. The ML/TF risk in the cross border sector is higher where

¹²⁸ Central Bank of Ireland's 2014 Insurance Statistical Review, <https://www.centralbank.ie/publications/Pages/statistics-research.aspx>

¹²⁹ Includes Life Insurance undertakings authorised by the Central Bank or authorised by another EEA Member State and operating in Ireland under the EEA passporting regime

distribution networks are spread across more jurisdictions and where products are distributed in non-EEA jurisdictions where AML/CFT regimes are not equivalent to those within the EEA.

The physical distance between these insurers and their intermediaries (especially in the case of services provided under 'Freedom of Services', with no physical presence in the target market) presents a higher ML/TF risk, as insurers need to rely on intermediaries to conduct adequate CDD on their behalf. In addition, insurers' ability to adequately vet intermediaries and to exercise oversight of controls carried out by intermediaries' increases the risk in this sector.

The wider geographic reach of cross border insurers increases the likelihood of their exposure to PEPs and other higher risk customers which increases the ML/TF risk.

Overall Risk – Domestic & Cross-Border Life Assurance

The ML/TF risk for the life insurance sector is assessed as **Medium Low** because many of the products offered by this sector do not offer sufficient flexibility to be attractive to money launderers or terrorist financiers for example, protection only or pension products. The potential risks presented by intermediate or higher risk products such as single premium investment products, which may offer cash surrender value or permit partial surrender during the term, can be mitigated both by the due diligence conducted at the outset of and during the business relationship and also the controls in place at the point of claim or encashment when each policy is subject to additional scrutiny. While the cross border life insurance sector can present higher risk due to the physical distance from its target market and intermediary network, many insurance firms mitigate this risk by repatriating due diligence documentation and information and conducting their own oversight and monitoring. In addition many of these Irish life insurance firms are owned by a credit institution in another EEA Member State and distribute their products through the branch network of the parent company, which is required to operate equivalent AML/CFT controls. This further mitigates the risks associated with the cross border life insurance activity.

Funds/Funds Administrators

The funds sector is an important part of the Irish financial services industry, both in terms of assets under management and the number of investors in Irish funds or in funds supported by Irish Fund Service Providers. As at the end of 2014, the total value of assets domiciled or administered in Ireland exceeded €3.2 trillion, with over €1.66 trillion relating to Irish domiciled funds¹³⁰.

While there are many different actors in the Irish funds industry, the main vulnerability of this sector to ML/TF risk lies predominantly with the funds and the fund administrators. The fund is both the entity and the central product on which the funds industry is based. The fund also has the direct customer relationship with the fund investor. However, it is important to recognise the significant role played by the fund administrator in the relationship between the investor and the fund. It is the fund administrator who is the gatekeeper to the fund. The fund administrator is the point of contact in the client relationship between the investor and the fund and it is the administrator who provides the AML/CFT capability to the fund to discharge its legal obligations. For these reasons the overall ML/TF risk associated with fund administrators is higher than other fund service providers who have similar risk exposure to the funds to which they provide services.

As such, this section focuses on the ML/TF risk for funds and fund administrators.

Overview - Funds

Depending on the nature of a fund, investors are free to sell or redeem their shares/units at any time (open ended fund) or at a defined period (close ended fund). Funds may have high volumes of subscriptions

¹³⁰ Department of Foreign Affairs and Trade, Minister Flanagan addresses the Irish Funds Industry Association seminar in Zurich, May 2015, <https://www.dfa.ie/news-and-media/press-releases/press-release-archive/2015/may/ministerflanaganaddressesirishfundsindustryassociationseminarinzurich/>

and redemptions by investors either at specific points in time (close ended) or on an on-going basis (open ended).

While a fund is a legal entity and a designated person in its own right, most of its operations and activities are conducted under contractual arrangements by a variety of supporting funds service providers (FSPs) including fund administrators, promoters, asset managers, depositories, distributors and fund managers.

Main Vulnerabilities

The often complex legal structure of funds can raise the ML/TF risk in the sector due to the lack of transparency of ownership and control associated with these complex structures. These opacities can be compounded where a fund's bank and custodian accounts are held in offshore jurisdictions, particularly those with stringent bank secrecy laws. As a result, it can be difficult to establish the source, destination and purpose of funds raised.

The broad and diverse investor base within the funds industry raises the ML/TF risk due to the fact that the investor base can include:

- small retail clients;
- high net worth individuals;
- PEPs;
- cash based businesses;
- complex-structured corporate customers;
- charities; and
- regulated institutions.

Customers with complex ownership structures are a particular feature of the funds industry. The complexity of certain corporate investors, investments from holding companies based in off-shore jurisdictions and nominee investments can increase the difficulty in establishing the ultimate beneficial ownership of invested monies.

The reliance on other regulated third parties by funds and fund administrators is also prevalent in this sector. Funds and fund administrators sometimes rely on letters of comfort or letters of introduction from regulated entities to identify and verify investors subscribing to a fund. This risk is further increased where the fund or fund administrator does not have adequate oversight of the effectiveness of the controls that the regulated third party employs. It is also common for investors to invest in a fund via a regulated intermediary. The reason for this is that the customer already has a business relationship with the intermediary who recommends investing in the Fund. As a result however, there is rarely face to face contact between the investor and the fund or fund administrator.

The Irish funds industry is significant in scale and is international in nature. Certain Irish funds benefit from a European "passport" and can be sold in any other EEA Member State without the need for any additional authorisation. Many funds are marketed and sold internationally.¹³¹

Fund Administrators

Overview

Funds appoint a fund administrator, under an outsourcing arrangement, to handle the day-to-day back office operations of a fund. As such, the client of the fund administrator is the fund itself. Client relationship managers from the fund administrator will meet face to face with representatives of the fund at initial on-boarding and indeed throughout the customer relationship.

Fund administrators typically coordinate with other FSPs in providing services to Irish domiciled and non-Irish domiciled funds. As at 30 April 2016 there are approximately 35 fund administrators authorised by the Central Bank ranging in size from the very large firms, which are part of global groups with billions of assets under management, to smaller stand-alone entities providing more 'boutique' fund administration

¹³¹ Ireland: A Guide To International Fund Distribution, Irish Funds, June 2015

services to a specific customer base. Ireland is the largest fund administration centre in the world. For example, over 40% of global hedge fund assets are administered here¹³².

Main Vulnerabilities

Some of the services outsourced to the fund administrator by the fund are more vulnerable to ML/TF risk. Such services include:

- carrying out of CDD to establish the identity of investors;
- processing the movement of investor monies by EFT in and out of the fund; and
- maintaining shareholder registers to reflect changes and transfers in investor shareholdings.

There has been an increasing trend of fund administrators themselves outsourcing certain back office functions, including the processing of initial and on-going CDD and transaction monitoring, to group subsidiaries or third parties in lower cost jurisdictions. Often such entities may not be regulated in their home jurisdiction as the fund administrator remains responsible for the outsourced function. This further outsourcing, by its nature, adds extra layers to the process and may remove direct onsite compliance and oversight presence.

Irish fund administrators provide services to both Irish domiciled funds and non-Irish domiciled funds. Irish and EU domiciled funds are required to comply with common transparency and prospectus requirements while non-EU domiciled funds may not be subject to equivalent regulatory requirements. Such non-EU domiciled funds include funds domiciled in jurisdictions that have stringent bank secrecy legislation and also in jurisdictions traditionally considered to be tax havens. This increases the difficulty in determining the beneficial ownership of the fund, as well as the ML/TF risk.

Overall Risk – Funds industry

The ML/TF risk for the Funds industry is assessed as **Medium-High**. The funds industry in Ireland has a diverse legal and operational structure. The funds industry is not cash based, unlike retail banks and money remitters. There is, however, a wide geographical reach both in terms of the jurisdictions into which Irish funds are marketed and also in terms of the non-Irish funds to which fund administrators may provide services. The customer base for funds themselves is broad including complex legal structures. Such complex structures can result in challenges in establishing the beneficial ownership. There are high volumes of transactions (i.e. subscriptions and redemptions) associated with certain types of funds. Funds are usually marketed through distributors and do not have direct business relationships with the underlying investor. There is a high level of outsourcing in the sector and significant reliance on third parties to conduct CDD.

While ultimate responsibility for AML/CFT controls remains with the fund, the fund administrator provides much of the AML/CTF control framework for the fund to discharge its responsibilities under the CJA 2010.

Asset Managers

Overview

As at 30 April 2016 there were approximately 77 Asset Managers authorised by the Central Bank. Asset management services typically comprise the provision of professional management and trading of securities and other types of assets to achieve a specific investment strategy agreed with the customer in advance in a discretionary mandate. This section focuses on firms for which asset management is their main business although it must be noted that many investment firms include asset management as part of a broader product and service offering to customers.

Main Vulnerabilities

An asset manager's customers may range from natural persons to more complex corporate legal structures and trusts. Customers with complex ownership and corporate structures increase the difficulty in identifying ultimate beneficial ownership. This, in turn, increases the ML/TF risk associated with these customers

¹³² Irish Funds, Getting Started in Ireland: Why Ireland, <http://www.irishfunds.ie/getting-started-in-ireland/why-ireland>

although this risk is somewhat mitigated by the substantial information required from customers at the outset regarding their sources of funds and risk appetite in order to provide this service. In addition, the risk is further mitigated due to the typical nature of business relationship in the asset management sector. These relationships are typically longer term and range from 5 years to over 20 years.

Typically there is direct face to face engagement between asset managers and their customers at time of on-boarding and/or throughout the business relationship to gain an understanding of the customer's investment objectives. However, engagements are also facilitated through electronic media or phone. Some asset managers may target customers by routing their products and services through accountants and regulated institutions such as retail intermediaries and other investment firms.

Asset managers generally do not accept cash from clients and do not facilitate once off transactions by clients nor pay-outs to third parties. Monies are transferred predominantly via Electronic Fund Transfer, although occasionally by cheque in respect of retail customers. In addition, asset managers providing services to the funds and pensions sectors typically do not hold client assets themselves. Others may provide safe custody arrangements for retail and high net worth clients.

While Irish asset managers have a broad geographical reach, the Central Bank of Ireland understands that the majority of services provided by this sector are provided within the EEA. This reduces the ML/TF risk associated with operating across a broad geographical base due to a decreased likelihood of connection to a higher risk jurisdiction.

Overall Risk

The overall ML/TF risk for the Asset Management sector is assessed as **Medium-Low**. While there are high levels of assets under management and high value transactions, services tend not to be cash based, facilitate once off transactions or pay outs to third parties. The customer base can include complex or non-resident corporate entities and trusts. However, associated customer risks are somewhat mitigated by the substantial information required from customers in order to provide this service. Also, the nature of the service means that business relationships are long term in nature. Services are provided predominantly face to face, either directly or through intermediaries.

Investment Firms other than Asset Managers

Overview

As at 30 April 2016 there were a total of 27 Investment Firms other than Asset Managers authorised by the Central Bank. There is a broad range of investment firms within this sector. Some firms are standalone, offering a narrow range of services to a limited customer base, while others are large institutions who are members of multi-national groups offering a broad range of services which may include stockbroking, asset and/or wealth management, and corporate finance. Customer numbers generally depend on the type of services being offered. Some investment firms may execute high volumes of transactions for a substantial customer base on a daily basis.

Main Vulnerabilities

The ML/TF risk to investment firms varies according to the particular business model of a firm. This is due to the wide diversity of products and services offered within the sector. These products and services carry varying degrees of ML/TF risk including a number of higher risk services such as:

- Trade execution services which can facilitate anonymous or high speed trading;
- Wealth management services; and
- Corporate financing activities.

However, the majority of firms typically offer services that are neither cash-based nor provided on a once-off basis. Generally, monies are transferred via Electronic Fund Transfer, or by cheque in limited circumstances. These factors decrease the risk associated with higher risk products and services, where offered.

Similar to asset managers, the customer base for other investment firms covers a very broad spectrum of natural persons, charities and legal and corporate entities, including potentially high net worth individuals, customers with complex legal structures, and trusts. The complexity of certain corporate customers can pose challenges in ascertaining beneficial ownership, which increases the ML/TF risk posed.

The level of customer interaction between investment firms and their customer varies according to the service offered. While the traditional investment firm operating model relies on the personal relationship between the investment firm and customers, the emerging trend towards online execution only brokerage services removes the face to face interaction and, in turn, increases the money laundering risk. At present, this risk is somewhat mitigated by the fact that such online services are currently only offered by a small number of larger firms, although a future increase in adoption on online services will increase the overall risk for the sector.

The geographical reach of Irish investment firms is broad. While a portion of services are carried out internationally, especially firms operating in the corporate finance space, most services are provided within the EEA.

Overall Risk

The overall ML/TF risk for investment firms is assessed as **Medium-High**. This risk rating has been assigned due to the range and breadth of services provided by investment firms, a number of which could be considered of a higher vulnerability to ML/TF risk. For the larger firms, transaction volumes and customer numbers are high. The customer base covers a broad spectrum of natural persons, charities, trusts and corporate entities. While delivery channels vary considerably across the sector, many products and services can be provided electronically or over the phone. However, services are predominantly provided directly by the investment firms themselves, however the use of intermediaries to provide services is a feature of this sector. Finally, while services are carried out on an international basis, most services are provided within the EEA and therefore geographic reach is more limited than in other sectors.

Credit Unions

Overview

Credit Unions are member-owned, not-for-profit, financial cooperatives that provide savings, loans and other financial services to their members. Members of a credit union are united by a common bond such as a particular location or profession which influences the customer and geographic bases of Credit Unions. Credit Unions provide a localised service and have a presence in every county in Ireland. Services are not offered to the public at large. Due to the local nature of Credit Unions, the sector is highly fragmented although in recent years there has been a trend towards consolidation in the sector which has seen the common bond in some cases widening significantly.

As at 30 April 2016 there were 341 Credit Unions authorised by the Central Bank. The Credit Union sector has over 3.3 million members, with combined savings of over €12 Billion and total assets of over €14 Billion.¹³³

Main Vulnerabilities

The cash intensive nature of Credit Unions' main services, savings and loans, increases the difficulty in identifying source of funds increasing the risk that the proceeds of crime are being used to repay loans or to accumulate into larger savings sums. A small number of Credit Unions offer additional cash intensive services, such as foreign exchange and money remittance, which increases the ML/TF risk in these Credit Unions.

¹³³ See ILCU Factsheet: <http://www.creditunion.ie/whoweare/>; ILCU Oireachtas submission: <http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/committeetakes/CHH2016050500002#LLL00100>; and Central Bank Statement <https://www.centralbank.ie/press-area/speeches%5CPages%5CIntroductorystatementbytheRegistrarofCreditUnionsAnneMarieMcKiernanatheOireachtasCommitteeonFinancePublicExpenditureRef.aspx>

The member base of Credit Unions predominantly consists of natural persons resident in Ireland, the majority of whom live or work in close proximity to their Credit Union. Many community Credit Unions are quite small in size and members tend to be well known to staff, which decreases the risk of money laundering due to the personal relationship with the customer. However, where Industrial and Occupational Credit Union membership is drawn from a profession or employer, staff do not typically establish the same personal relationship with customers. This increased risk due to the weaker personal relationship is mitigated by the fact that accounts are typically funded directly from customer salaries making them easily identifiable.

Credit Unions' member base has expanded to include sole traders, partnerships, small corporates, clubs and societies. This has exposed credit unions to cash intensive businesses thereby increasing the overall customer risk profile, for example where individuals use their personal accounts to lodge business proceeds but CDD has not been conducted on that business.

Credit Unions do not have an international branch network although the branches situated close to the border counties may be more vulnerable to ML or TF.

In most instances credit union services are provided directly to the member on a face to face basis which lowers the ML/TF risk. However, there is an emerging trend towards the online provision of services within the credit union sector which means that the face to face element of the transaction will be lost. Online services are provided by a minority of credit unions but this number is increasing and will, in time, increase the overall ML/TF risk.

While transaction monitoring is generally conducted manually, which increases the ML/TF risk, Credit Unions have begun implementing improvements to their IT systems which will enable more effective transaction monitoring to be conducted in the future and in turn reduce the ML/TF risk.

Overall Risk

The overall ML/TF risk in the Credit Union sector is assessed as **Medium-Low**. Credit Unions generally provide a particularly localised service to natural persons who are within a common bond (either on the basis of where they live or where they work), accordingly reducing the geographic reach and assisting with understanding the type and nature of a credit union's customer. However, there are large amounts of cash transactions within the sector and as credit unions amalgamate and services move online the face to face element of their services may be lost which could make customer due diligence more challenging for the sector.

Moneylenders

Overview

As at 30 April 2016 there were 40 firms licensed by the Central Bank to carry out moneylending activities in Ireland. Moneylending firms are licensed on an annual basis.

The credit provided will generally be in the form of a cash loan. However, it may also involve goods being provided on credit from a retailer or the purchase of goods from a catalogue. The moneylending firms in operation in Ireland can be divided into four categories on the basis of the product or service that they offer. These are:

- Home collection firms;
- Remote firms;
- Retail firms; and
- Other firms, including catalogue firms.

Main Vulnerabilities

The majority of moneylenders' customers are individuals from distinct localities with which the moneylender is familiar. Many moneylenders typically have established relationships with their customers which may span many generations and many new customers are referred by already existing customers. In general,

moneylenders have good knowledge of their customers, they are in a good position to identify the source of wealth and funds.

However, due to the personal nature of customer relationship a moneylender may be more likely to accept the customer's information without looking for further proof or verification on the source of funds and wealth.

Due to the cash intensive nature of moneylenders' business there is a risk that low-level proceeds of crime may be used to repay credit advanced by moneylenders. This risk is somewhat mitigated by the fact that the early repayment of loans to facilitate money laundering would undermine the moneylending business model and moneylenders will typically not advance further credit to individuals who have repaid advanced credit substantially ahead of schedule.

Overall Risk

The ML/TF risk for the moneylending sector is assessed as **Medium Low**. The moneylending sector is traditionally associated with high volumes of cash transactions which would typically increase ML/TF risk; however the cash amounts involved are relatively low. ML/TF risk is also mitigated by a limited product offering being predominantly credit extended to facilitate the purchase of white goods/clothes and relatively small cash loans. Geographic risk is low as moneylenders typically operate in their local area. Customer risk is also low as the customer base is predominantly natural persons as opposed to corporates or complex legal entities and moneylenders typically have a good knowledge of their customer base built up over long periods of time.

Trusts or Company Service Providers (Subsidiaries of Credit/Financial Inst.) (TCSPs)

Overview

As of 30 April 2016 there were 38 Trust or Company Service Providers, or 'TCSPs', that are subsidiaries of credit and financial institutions registered with the Central Bank. TCSPs are entities that, broadly speaking, provide services to form companies, or to provide registered offices or addresses for a body corporate or partnership. These activities also include any person who acts (or provides someone to act) as a trustee, nominee shareholder, partner, director, or secretary of a company/partnership.¹³⁴

TCSPs provide assistance to clients in the management of their financial affairs and as a result can significantly impact transactional flows through the financial system.¹³⁵ While TCSPs have many legitimate applications, such as tax planning, they can also be misused by criminals for purposes such as concealing the ultimate beneficial owner of funds, legitimatising the integration or layering of criminal proceeds within the financial system through various forms of investments. The activities of TCSPs are of a higher risk when the services are provided internationally and where the customers are based in higher risk jurisdictions.

Main Vulnerabilities

The parent companies of all Central Bank authorised TCSPs are regulated entities and are subject to prudential and AML/CFT supervision by the Central Bank of Ireland. The services provided by these TCSPs are generally ancillary to the services already offered by their parent firm to the same Irish based customers. Interactions with these customers are led by the parent and are subject to the parent's AML policies and procedures. Services typically offered by TCSPs authorised by the Central Bank of Ireland are for the purpose of:

- Providing corporate employers with trustee services for their Revenue Approved Occupational Pension Schemes on behalf of their employees;
- Acting as pension trustee to Small Self-Administered Pension Schemes (SSAPS);
- Acting as the trustee of exempt unit trusts; and
- Acting as nominee shareholder for persons who also have a relationship with their parent.

¹³⁴ Section 24(1), Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

¹³⁵ FATF Report 2010, Money Laundering using TCSPs

While a number of these services, such as acting as a nominee shareholder, are generally considered to be a higher ML/TF risk the risk is mitigated by the fact that TCSPs authorised by the Central Bank of Ireland are subsidiaries of regulated entities.

Overall risk rating

The overall ML/TF risk for Central Bank authorised TCSPs is assessed as **Low**. TCSPs within the remit of the Central Bank are offering such services as an ancillary part of products and services already provided to customers of their regulated parent company. These customers are predominantly based in Ireland and are not within traditionally higher risk categories although they are typically “high net worth individuals”.

Retail Intermediaries

Overview

As at 30 April 2016 there were approximately 2,000 retail intermediaries, or brokers, in Ireland that fall within the scope of Irish AML/CFT legislation. There are a variety of retail intermediary firms operating in Ireland ranging from subsidiaries of large multinational insurance companies and credit institutions to small owner-operated firms. On the basis of number of employees employed in the sector, most firms are small (with 89% of firms having between one and ten employees)¹³⁶ to medium size.

Retail intermediary business is based on direct long term business relationships with their clients and majority of business is conducted on a face-to-face basis. Most clients are Irish resident and commonly have been introduced by already existing client and most retail intermediary firms in Ireland have less than 1,000 customers.

The majority of firms in this sector are primarily involved in the provision of financial products which originate from another authorised credit or financial institution such as a retail bank, insurance company or investment management firm. Commonly, the types of products arranged by retail intermediaries are life assurance, pensions, permanent health insurance, critical illness cover and investment products.

Main Vulnerabilities

Retail intermediaries generally have good knowledge of their customers and they meet them regularly on a face-to-face basis. However, due to the personal nature of customer relationship, there is a risk that a retail intermediary may be more likely to accept the customer’s information without looking for further proof or verification on the source of funds and wealth.

There is also a risk that retail intermediaries could collude with their customers to facilitate ML/TF. However, such risk is reduced through the oversight exercised by the relevant insurance company or investment firm who is providing the product to the customer.

Overall Risk

The overall ML/TF risk for the retail intermediary sector is assessed as **Low**. While the retail intermediary customer base can be quite diverse and potentially include customers considered ‘high risk’ - e.g. high net worth individuals - in general, retail intermediaries are not involved in handling any customer monies thereby significantly reducing the ML/TF risk.

¹³⁶ Central Bank of Ireland, Report on the Retail Intermediary Sector in Ireland, February 2013, <http://www.centralbank.ie/regulation/industry-sectors/retailintermediaries>

Non-Financial Sector

7

Non-Financial Sectors

Overview

The regulated non-financial sector commonly known as ‘Designated Non-Financial Businesses and Professions’, or ‘DNFBPs’, covers businesses and professional services that are also ‘designated persons’ for the purposes of Ireland’s AML/CFT regime. A broad range of DNFBPs operate in Ireland and are identified in Section 25 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as follows:

- Private Members’ Clubs at which gambling activities are carried on;
- Dealers in High Value Goods (*specifically those who may receive payments in cash of at least €15,000 whether in a single transaction or in a series of linked transactions*);
- Trust or Company Service Providers;
- Independent Legal Professionals (Barristers and Solicitors);
- Notaries
- Property Service Providers;
- Auditors, Tax Advisers, and External Accountants.

The DNFBP sector in Ireland is both broad and diverse, falling as it does under the AML/CFT supervision of 12 competent authorities. The competent authorities are:

- The Law Society of Ireland for solicitors;
- The General Council of the Bar of Ireland for barristers;
- Nine designated accountancy bodies;¹³⁷ and
- The Minister for Justice and Equality for all other DNFBPs.

This section of the National Risk Assessment sets out Ireland’s understanding of the ML/TF risks present in the Irish non-financial sector. In addition to considering the relevant ‘designated persons’ identified in the Act, this section also considers the ML/TF risks present in the following sectors:

- Gambling and
- Non-Profit Organisations.

¹³⁷ ACCA, the Association of Chartered Certified Accountants; AIA, the Association of International Accountants; CIMA, the Chartered Institute of Management Accountants; CIPFA, the Chartered Institute of Public Finance and Accountancy; ICAEW, the Institute of Chartered Accountants in England and Wales; ICAI, the Institute of Chartered Accountants in Ireland; ICAS, the Institute of Chartered Accountants of Scotland; ICPAI, the Institute of Certified Public Accountants in Ireland; and IIPA, the Institute of Incorporated Public Accountants

Private Members' Clubs (PMCs)

Overview

The Private Members' Club, or 'PMC', sector consists of clubs where gambling activities are carried on. Persons directing Private Members' Clubs are 'designated persons' under the Act and must register with the Anti-Money Laundering Compliance Unit, the 'AMLCU', in the Department of Justice and Equality, for money laundering compliance purposes. Irish PMCs range from small to large scale establishments and offer a variety of gambling activities to members. The vulnerability of individual PMCs to money laundering varies according to a range of factors including the size of the PMC, the activities offered, and spend in excess of the threshold of €2,000¹³⁸.

As at 1 May 2016 there were a total of 42 PMCs registered with the AMLCU, all of which have/will be inspected for AML/CFT compliance in 2016. The AMLCU conducts an initial once-off daytime inspection on new PMCs registered to review the Club's policies, procedures and staff training. This is followed by a night-time operational inspection for the purpose of conducting an inspection of all records maintained by the PMC including CDD and transaction records. The intensive inspection regime along with the provision of continuing advice and guidance on all AML/CFT matters has led to significant improvements in the measures implemented by PMCs in recent years. This has resulted in an overall reduction in the vulnerability of PMCs to money laundering.

Main Vulnerabilities

PMCs are highly cash intensive businesses with the potential for significant amounts of cash to be wagered on a nightly basis in a given establishment resulting in a high turnover of cash. Evidence suggests that the gambling pattern of larger PMC customers is between €1,000 and €10,000 wagered per night, with high spend customers exceeding this amount. For these reasons, the cash intensive nature of PMCs increases the risk of their use for money laundering or terrorist financing.

Most PMCs offer patrons the opportunity of one grace visit. An individual going to a PMC on a grace visit is required to complete a member's application form for attendance tracking purposes. It is often the case that the individual would not have any identification document on them. An individual attending the PMC on a grace visit will only be entitled to spend up to the threshold of €2,000. Where the individual has winnings in excess of the threshold of €2,000 the individual must provide identification before winnings over €2,000 can be collected.

The following customer types potentially present an increased risk of money laundering:

- Customers who visit infrequently yet gamble large sums of money. The higher risk due to the large sums of money is somewhat mitigated in PMCs where owners know their customers;
- Customers who cash in for chips for large sums of money but only spend a small amount of that money and then request the remainder of the cash submitted along with any winnings to be given back by way of a winner's cheque;
- Regular customers who gamble large sums of money. This is higher risk due to the large sums involved; and
- Frequent customers who unexpectedly gamble significantly in excess of their normal amounts. This is a higher risk where tracking of re-cycled spends is inadequate.

The diverse customer base of PMCs increases the risk of money laundering as it has been known to include:

- Ex-criminals;
- Domestic and foreign politically exposed persons; and
- A high proportion of non-EU customers which increases the risk of foreign criminal gangs engaging in third party laundering through these customers.

¹³⁸ As per the 3rd Anti-Money Laundering Directive

Given the nature of PMC businesses, there is an increased risk that suspicious activity may be overlooked and not reported, in particular due to the perceived negative impact on their business. Suspicious transaction report statistics for 2015 indicated that less than 1% of all STRs reported were raised by PMCs.¹³⁹

PMCs offer a range of activities which include:

- Live gaming, such as Blackjack, Roulette and Punto Blanco, which are considered more vulnerable to money laundering as individuals could, for example, collude to launder money by hedging their bets; and
- Poker tournaments, which are considered to be less vulnerable to money laundering due to the fact that people compete to win structured cash prizes per tournament.

PMC staff are not vetted by An Garda Síochána although the risk is somewhat mitigated by the strict vetting procedures for persons being taken on as employees and the training provided by PMCs to staff members. There is a heavy dependency on staff integrity and ability to identify and report suspicious behaviour.

Overall Risk

The overall ML/TF risk within the Private Members' Club sector is judged to be **Medium-High** due to cash intensive nature of PMC business, the nature of the products and services offered, the potential exposure to high risk customers and the lack of information in respect of source of wealth. Improvements in AML/CFT activities within this sector as a result of increased engagement between the AMLCU and PMCs, have reduced the overall risk for the sector over recent years.

High Value Goods Dealers (HVGDs)

Overview

The Act defines High Value Goods Dealers, or 'HVGDs', as any person trading in goods that accept cash payments of €15,000 or more in a single transaction or in a series of linked transactions or apparently linked transactions. Where this threshold is reached, the HVG D must apply CDD measures to such transactions, retain adequate records of transactions and report any suspicious transactions, if detected. The Sales records maintained by HVG Ds must include the method of payment and all records must be kept for a period not less than 5 years. There are many businesses and individuals that fall into this category including garages, jewellers, art and antique dealers, boat dealers and plant machinery sales. The AMLCU has a record of some 1,230 HVG Ds across a variety of business types. HVG Ds are not required to register with the AMLCU and are identified on a continuous basis by the AMLCU as their existence is discovered through intelligence gathered.

The AMLCU conducts risk based inspections of HVG Ds and inspected some 397 HVG Ds in 2015. The AMLCU collaborates with law enforcement authorities in respect of intelligence concerning ML/TF suspected to occur in HVG Ds and is committed to improving its inspection and compliance activities by proactively inspecting new HVG D sectors that emerge. Law enforcement authorities and the AMLCU are committed to deepening their knowledge in this area.

¹³⁹ Financial Intelligence Unit, An Garda Síochána

Main Vulnerabilities

The accessibility and cash intensive nature of transactions in this sector increases its vulnerability to money laundering as an individual who wishes to dispose of illicit funds could simply purchase a high value good, on an anonymous basis, with cash or seek a third party to purchase the item on their behalf to further anonymise the transaction. The majority of HVGDs accept cash payments. The risk is somewhat mitigated for car purchases given that cars are registered by the owner rather than the purchaser.

While HVGDs are required to conduct CDD on customers who purchase goods for €15,000 or more in cash, inspections suggest that not all HVGDs are aware of their AML/CFT obligations. In addition, HVGDs that are aware of their obligations may fail to ensure that adequate CDD is carried out.

Challenges in detecting linked transactions that exceed €15,000 (due to the lack of customer and transaction tracking systems) increases the ML/TF risk. It is the experience of Authorised Officers conducting inspections that making numerous purchases close to, but below, the €15,000 threshold may be a common strategy to conceal the laundering of illicit proceeds. This is facilitated by:

- Weaknesses in AML/CFT procedures across a range of entities in the HVGD sector, such as the lack of monitoring of linked transactions; and
- The relatively high threshold amount which can allow significant sums to be quickly laundered.

Given the local nature of many HVGD businesses, there is an increased risk that any detected suspicious activity will be overlooked and not reported due to the perceived negative impact on their business. STR statistics for 2015¹⁴⁰ indicated that less than 1% of all STRs reported were raised by HVGDs.

HVGDs deal in a range of luxury goods and products that make them vulnerable to ML/TF due to the highly portable nature and intrinsically high value of the goods and products. In addition, transactions with HVGDs are typically occasional in nature and will not result in business relationships being established with customers. Products sold by HVGDs include:

- Cars, which are considered to be vulnerable to ML/TF due to the significant sums of cash accepted by car dealers, and the potential use of cars as payment instruments themselves. This has been confirmed by law enforcement intelligence;
- Jewellery, which is considered to be a lower ML/TF risk due to the lack of significant transaction volumes in those businesses;
- Boats, which are considered more vulnerable to money laundering due to the anonymous nature of boat ownership. There is no requirement to register boat ownership; and
- Plant and machinery, which is not considered to be a very high risk of money laundering as it is predominantly purchased by the agriculture and construction industries for commercial purposes.

Overall Risk

The overall ML/TF risk within the HVGD sector is judged to be **Medium-High**, due to the cash intensive nature of HVGD businesses, the nature of the products offered, and their high intrinsic value.

The 4th EU Anti-Money Laundering Directive which will be transposed into Irish law soon will reduce the HVG transaction threshold to €10,000. This will bring more transactions within the scope of AML regulation thus further reducing the vulnerabilities in this area.

¹⁴⁰ Financial Intelligence Unit, An Garda Síochána

Trust or Company Services Providers (Non-Financial) (TCSPs)

Overview

Trust or Company Service Providers, 'TCSPs', are entities that provide company or trust services to another company, in particular to facilitate the formation and operation of companies. There are currently some 300 TCSPs authorised by the Minister for Justice and Equality, as State Competent Authority for this sector.¹⁴¹ An authorisation is valid for a period of 3 years. The TCSP sector is diverse with a wide range of TCSPs providing a variety of services to companies.

TCSPs authorised by the State Competent Authority undergo a rigorous authorisation process where the beneficial owners and principal officers of a TCSP must undergo a fitness and probity assessment and must also be vetted by An Garda Síochána. TCSPs are inspected by the AMLCU at least once every three years on a risk-based approach. The AMLCU is committed to collaborating with other supervisors to enhance the cross-sectoral supervision of TCSPs.

While TCSPs are required by legislation to be authorised by the State Competent Authority, it is suspected that a number of entities offering trust or company services may be operating without such an authorisation. Operating as a TCSP without authorisation is an offence under the 2010 Act. The AMLCU is continuously striving to identify TCSPs that are operating without an Authorisation.

Main vulnerabilities

The complex services legitimately provided by TCSPs are attractive to those seeking to launder the proceeds of crime as they enable access to the financial system and can obscure the source of funds and the beneficial ownership of funds. Such services include:

- Acting or arranging for another person to act as a nominee shareholder of a company, which is considered to be high risk as money launderers could use the TCSP to buy or sell shares on their behalf thereby facilitating the introduction of illicit money into the financial system;
- Acting as a nominee director or secretary of a company, which is considered high risk as the identity of the TCSP's client is obscured from the Companies Registration Office, the 'CRO'. The TCSP might unknowingly discharge their obligations in these roles in accordance with the instructions of a criminal client;
- Providing registered office or business address facilities is considered higher risk where the TCSP is not providing other TCSP services to a client (i.e. no other business relationship). The lack of interaction between the TCSP and the customer may lead to a difficulty in detecting suspicious activity;
- Providing trust services which can vary from low risk to high risk, depending on the nature of the trust. Trusts might vary from lower risks trusts, such those established by parents for the benefit of children or vulnerable individuals, to more complex structures, where the source of trust funds is unclear;
- The establishing of complex corporate structures and corporate vehicles may increase the risk of money laundering in more complex corporate structures, or where the TCSP acts or arranges for someone to act as a nominee shareholder, as the beneficial owner and true source of funds is obscured. This could facilitate the introduction of illicit proceeds of crime into the financial system.

¹⁴¹ In this section of the NRA, the term 'State Competent Authority' is taken to refer to the Minister for Justice and Equality in regard to TCSPs not regulated within the financial sector.

The international nature of the TCSP sector may expose parts of the sector to a higher risk of money laundering. This is because:

- Customers may be from high risk jurisdictions;
- The business relationship may not be face to face e.g. by email or phone call;
- TCSPs may be unable to verify CDD documentation as true originals due to the remote nature of the business relationship; and
- TCSPs may sometimes rely on third parties to carry out due diligence on their behalf.

Overall Risk

The overall ML/TF risk within the TCSP sector is judged to be **Medium-High** due to the nature of the services offered by TCSPs, the potential exposure to high risk jurisdictions and customers, the sometimes lack of face to face contact with customers on establishing the business relationship, the challenges in effectively monitoring customer activity and the lack of transparency with respect to the beneficial ownership of shares in companies. However, these risks are somewhat mitigated by the rigorous authorisation process undertaken by the State Competent Authority before commencing business and the approach taken to TCSP inspections.

The transposition of the beneficial ownership provisions of the 4th EU Anti-Money Laundering Directive will help to mitigate some of the risks in this area by providing for greater transparency in the beneficial ownership of legal vehicles.

Notaries

Overview

A Notary Public is a public officer constituted by law to serve the public in non-contentious matters usually concerned with foreign or international business. A Notary is empowered by law and by custom and usage of notaries through the ages to:

- Administer Oaths
- Attest signatures
- Authenticate documents
- Give Notarial Acts
- Take Affidavits (though not for use in courts in Ireland)
- Take Affirmations and Declarations
- Receive and make protests under Mercantile Law and issue notarial certificates in respect of documents and persons
- Draw up powers of Attorney and other legal documents customarily prepared by Notaries Public.

The Faculty of Notaries Public in Ireland is an incorporated body limited by guarantee, incorporated in Ireland on the 13th March 1981, having as its objects the promotion, advancement and regulation of the profession of Notary Public in Ireland. The Faculty provides information to Notaries Public, Solicitors and the public in general on matters within its province and in particular as regards aspects of notarial practice and procedure in Ireland.

Entry to the Profession of Notary Public for suitably qualified candidate notaries is through the completion of the Diploma in Notarial Law & Practice, although successful completion of the Diploma does not guarantee appointment as a Notary Public. In addition, candidates must be practising solicitors or barristers with post-qualification experience in the general practice of law. Furthermore, appointment as a Notary Public involves a formal Petition to the Chief Justice of Ireland in open Court of a Notice of Motion.

Where a candidate notary is an employed solicitor, including an in-house counsel for a corporation, or a partner in a law firm, a further requirement is a letter from the relevant employer's Chief Executive Officer, or managing partner, consenting to the relevant candidate notary proceeding with the Petition. An employed candidate notary or a partner in a law firm must also undertake never to notarise documents for his/her employer or law firm and there is a corresponding undertaking required from the firm/corporation never to seek notarial services in connection with a matter in which the employer/corporation is involved. Barristers are not permitted by the Bar Council to practise as a notary from a desk in the Law Library. The Bar Council also requires barristers to keep fees earned as a barrister separate from notarial fees.

Notaries in common law jurisdictions are not as central to land transactions as they would be in civil law jurisdictions. There are presently 230 Notaries practicing in Ireland. To date the State Competent Authority has not undertaken any inspections of this sector. Inspections will shortly be scheduled to establish the risk levels pertaining to this sector.

Overall Risk

There are a limited number of notaries practicing in Ireland and, the entry to the Profession of Notary Public is a rigorous process. As the State Competent Authority has not yet undertaken any inspections of this sector, it is challenging to fully assess the overall risk of this sector. The overall ML/TF risk for notaries is assessed to be **Medium-Low** until a full understanding of this sector is established.

Property Services Providers

Overview

Property Service Providers (PSPs) are required to be licensed by The Property Services Regulatory Authority (PSRA) on an annual basis. The PSRA is the statutory authority with responsibility for licensing property services providers in Ireland, as defined under Section 2 of the Property Services (Regulations) Act 2011. While the Minister for Justice and Equality is presently the Competent Authority for this sector, it is the Minister's intention to appoint the PSRA as the State Competent Authority for the PSPs in September/October 2016. The services which are within the scope of the Act are provided mainly by Auctioneers and Estate Agents. These are:

- (a) Auction of property other than land; and
- (b) Purchase or sale, by whatever means of land.

At present, there are approximately 5,700 PSP licensees. This includes approximately 1,800 businesses (e.g. Employers) with approximately 3,900 individuals licensed to carry out property services. The residential property price register indicates that there were 48,511 residential property transactions in Ireland in 2015, worth over €10 billion.¹⁴²

Property transactions generally require the involvement of financial institutions and legal professionals, both of whom are also designated persons under the Act. PSPs do not generally handle the large sums of money typically involved in property transactions. PSPs only handle a small percentage of the overall purchase price (typically between 1% and 2%), as a booking deposit, from which their fee is generally deducted and the balance transmitted to their client the vendor. Financial institutions and legal professionals generally handle the majority of property transaction proceeds.

The customers of PSPs are typically property vendors with whom PSPs complete a "Letter of Engagement" detailing the terms and conditions attaching to their business relationship with vendors, as required under the Property Services (Regulation) Act 2011. PSPs do not conclude a "Letter of Engagement" with property purchasers as they are not customers of the PSPs. The Act requires that PSPs undertake CDD on their

¹⁴² Property Price Register

customers, the property vendors, not the purchasers of properties. Legal professionals are required to conduct CDD on property purchasers where they have been engaged by purchasers to act on their behalf. In addition, where purchasers are customers of financial institutions those financial institutions are obliged to also conduct CDD on those customers.

The PSRA is committed to introducing a number of measures to enhance the AML/CFT regime across the PSP sector once appointed as the State Competent Authority. These include:

- Developing sector guidance;
- Introducing a mandatory AML/CFT continuous professional development (CPD) requirement;
- Discussion of AML/CFT at an industry representative forum; and
- Inclusion of AML/CFT obligations in PSP compliance audits.

Main Vulnerabilities

Notwithstanding the fact that PSPs' customers are property vendors and not purchasers, there are a number of vulnerabilities in PSPs which increase the ML/TF risk. These include:

- PSPs not undertaking adequate client due diligence of property vendors;
- Poor understanding of ML/TF;
- Poor understanding of their legal obligations under the Act;
- Inadequate identification of the legal owners of the property;
- Low level of Suspicious Transaction Reports;
- Potential for complicit PSPs in the selling and purchasing of property by criminals; and
- Commercial pressures between PSPs.

While concerns have been expressed regarding the low level of STRs from PSPs, there is minimal opportunity for PSPs to be used as a single vehicle to launder money without the involvement of other professionals. The PSP accepts a booking fee from the purchaser in the region of €5,000 to €10,000 depending on the value of the property or alternatively 1% to 2% of the value of the property. On successful completion of a sale, the PSP will deduct a professional fee and refund the remaining part of the booking deposit fee resulting in minimal funds exposed to potential money laundering. Separately, the purchaser will enter into a contractual agreement to purchase a property. This is usually with their solicitor, to whom a significantly large contractual deposit is paid. The solicitor will handle the completion of the purchase transaction and under the Act is required to undertake CDD.

PSPs generally do not deal in cash booking deposits, with some PSPs refusing to accept cash in order to reduce money laundering risk and to reduce the safety risks associated with handling large sums of cash.

Property transactions, where it is difficult to establish and verify the identity of the vendor, may increase the ML/TF risk, in particular where:

- there is no personal interaction with the customer, for example online auctions;
- the customer is resident in a high risk jurisdiction;
- the customer is a legal person such as a trust or a company;
- deposits are paid with third party cheques; and
- the property is offered for sale on behalf of a third party.

Overall Risk

Investment in real estate is viewed as an attractive means to launder the proceeds of crime and the low level of understanding and compliance with AML/CFT obligations increases the risk of money laundering. However, this risk is mitigated as PSPs do not handle significant sums of money and property purchase transactions are generally not possible without the involvement of other professionals. The overall ML/TF risk within the PSP sector is judged to be **Medium-Low**.

Legal Services Sector

Overview

Practising solicitors and barristers who provide certain legal services are ‘relevant independent legal professionals’¹⁴³ for the purposes of Ireland’s AML/CFT regime and are included within the definition of ‘designated person’¹⁴⁴ in the Act. The relevant services which bring solicitors and barristers within the scope of the Act are:

- a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:
 - (i) buying or selling land or business entities;
 - (ii) managing the money, securities or other assets of clients;
 - (iii) opening or managing bank, savings or securities accounts;
 - (iv) organising contributions necessary for the creation, operation or management of companies;
 - (v) creating, operating or managing trusts, companies or similar structures or arrangements;
- (b) acting for or on behalf of clients in financial transactions or transactions relating to land¹⁴⁵

Practising solicitors must hold practising certificates from the Law Society of Ireland (‘the Law Society’)¹⁴⁶ and barristers must generally hold practising certificates from the General Council of the Bar of Ireland (‘the Bar Council’) and be members of the Law Library.¹⁴⁷ These professional bodies are also the relevant competent authorities for AML/CFT purposes for their members.¹⁴⁸

There are approximately 2,200 firms of solicitors in Ireland providing legal services. Of the 2,200 firms of solicitors in Ireland, approximately 45% are sole practitioners, a further 25% have a single principal solicitor and the remaining 30% have 2 or more partner solicitors. Approximately 10,000 individual solicitors hold practising certificates in Ireland.¹⁴⁹ There are approximately 2,300 barristers in Ireland who are members of the Law Library.¹⁵⁰ There are also a small number of barristers who are not members of the Law Library.¹⁵¹ Barristers are all self-employed sole traders.

While barristers are designated persons for AML/CFT purposes, the overwhelming majority of barristers are not directly engaged by clients and do not seek them out. Barristers are independent advocates who rely on instructions from referring solicitors, they are required to maintain their independence at all times¹⁵² and owe an overriding duty to assist the Court in ensuring the proper and efficient administration of justice.¹⁵³

Barristers can generally only refuse to accept instructions where there is a conflict of interest or the barrister does not have capacity to accept the instruction. This is known as the “cab-rank rule.”¹⁵⁴ Due to the operation of the cab rank rule, the referral nature of the profession, and the overriding obligation owed by barristers to the court, barristers rely on the adequacy and effectiveness of solicitors’ AML/CFT measures as solicitors maintain the substantive relationship with, and conduct customer due diligence (CDD), on clients.

The wider legal services sector is an important contributor to the Irish economy, both directly and indirectly. More than 18,000 people were engaged in the sector in 2014 and it contributed an estimated €1.46

¹⁴³ Section 24, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

¹⁴⁴ *Ibid* Section 25(1)(d)

¹⁴⁵ *Ibid* Section 24(1)

¹⁴⁶ Sections 46, 54, Solicitors Act 1954

¹⁴⁷ Section 9, Code of Conduct for the Bar of Ireland, July 2014, (‘Bar Code of Conduct’)

¹⁴⁸ Section 60(2)(c) – (d), Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

¹⁴⁹ Information provided by the Law Society

¹⁵⁰ Information provided by the Bar Council

¹⁵¹ *Ibid*

¹⁵² Section 1, Bar Code of Conduct

¹⁵³ *Ibid* Section 2.2

¹⁵⁴ *Ibid* Section 2.14

billion to the Irish economy in 2014.¹⁵⁵ This was second only to the telecommunications sector in 2014.¹⁵⁶ In addition, the services provided by the legal services sector enable a significant amount of economic activity across the wider economy, in sectors such as real estate, financial services, aviation, technology and telecommunications.

The Law Society conducts approximately 400 on-site inspections per annum and employs a team of investigating accountants to conduct these inspections. The Law Society adopts a risk-based approach to selecting firms for inspection and takes into account a range of factors which may indicate potential risks, including:

- Previous supervisory experience of individual firms;
- Analysis of annual Reporting Accountant’s Report;
- Client complaints; and
- Professional indemnity insurance renewal delays.

The Law Society has observed a strong correlation between irregularities in a firm’s Reporting Accountant’s Report and the presence of inadequacies in that firm’s AML/CFT measures. As a result of its inspection activities, the Law Society files approximately 10 Section 63 reports per annum in respect of practising solicitors. Section 63(4) of the Act requires competent authorities, such as the Law Society, to inform An Garda Síochána and the Revenue Commissioners where they acquire information or form a suspicion that a person has been or is engaged in money laundering or terrorist financing.

The Law Society has published comprehensive AML/CFT guidance to raise Solicitors’ awareness¹⁵⁷ of their obligations under the Act. The guidance highlights risks and risk indicators specific to the legal services sector and is used by trainers and practitioners in the Society’s compulsory accounting and AML-compliance training modules¹⁵⁸. In addition, the Law Society recommends that solicitors identify all clients in all circumstances, even where the service provided is not within the scope of the Act,¹⁵⁹ so that solicitors can fully manage their customer risk profile.

The Law Society operates an AML/CFT helpline to assist practitioners in dealing with any arising AML/CFT issues. In addition, the helpline allows the Law Society to detect emerging trends and to respond in a proactive manner. The Law Society also has an AML Task Force which engages with a broad range of firms to further identify and address emerging AML/CFT issues. In addition, the Law Society regularly publishes information updates and bulletins to enhance solicitors’ awareness of their AML/CFT obligations and to draw attention to emerging issues.

Due to the nature of barristers’ profession, their reliance on the effectiveness of solicitors’ AML/CFT measures, and a lack of authority to inspect a member’s practise, the Bar Council does not monitor its members’ compliance with their AML/CFT obligations. However, the Legal Services Regulation Act 2015 will, when commenced, allow for the inspection of all legal practitioners, including barristers who are not members of the Law Library.¹⁶⁰

The Law Society and Bar Council are committed to continuously improving their AML/CFT supervision frameworks and are also committed to enhancing the awareness of AML/CFT obligations among legal practitioners. The Law Society and Bar Council are committed to improving the sharing of information and collaboration with other competent authorities and law enforcement authorities.

Main Vulnerabilities

The specialist nature of the knowledge and services provided by the legal services sector makes solicitors and barristers vulnerable to being sought out and exploited by criminals who seek to launder the proceeds

¹⁵⁵ Law Society of Ireland, *The Solicitors’ Profession: Contribution to the Irish Economy*, November 2014, p i

¹⁵⁶ *Ibid* p 6

¹⁵⁷ Law Society of Ireland, *Guidance Note for Solicitors on Anti-Money Laundering Obligations*, July 2010

¹⁵⁸ Solicitors (Continuing Professional Development) Regulations 2015 (S.I. No. 480 of 2015); operational from 1 January 2016; 3 hours on regulatory matters compulsory, 2 of which must be on accounting & AML compliance, <http://www.irishstatutebook.ie/eli/2015/si/480/made/en/print>

¹⁵⁹ *Ibid* para 6.4

¹⁶⁰ Section 39, Legal Services Regulation Act 2015

of crime or evade tax. This is because the involvement of legal professionals is necessary to complete certain transactions which are attractive to criminals.

Vulnerable services can include:

- Complicated financial and property transactions;
- Company and trust formations;
- Securities and funds transactions;
- Complicated cross-border transactions; and
- Establishing charities.

Due to the nature and potential scale of transactions associated with the vulnerable services offered, there is an increased risk that substantial proceeds could be laundered. This increases the risk of money laundering associated with these services.

Solicitors who regularly provide such vulnerable services may be at a higher risk of unknowingly facilitating money laundering through lack of identification of the true source of funds and the ultimate beneficial owner of funds. Involvement of the legal profession can be perceived as adding legitimacy to transactions.

Where solicitors obtain client money, they are obliged to segregate such funds from their own business funds by operating a separate client account. While a client accounts are an important and highly regulated,¹⁶¹ feature of solicitors' practises, if improperly managed, i.e. where inadequate or inconsistent CDD procedures are applied by a practise to its client account, there could be significantly heightened risk. Cases have occurred where solicitors' client accounts have been misused.

Barristers are prohibited from directly or indirectly administering or handling the funds, assets (including original title documents) of clients and also prohibited from giving financial advice in respect of such funds or assets.¹⁶² This restriction on the scope of barristers' services, to the provision of advocacy and legal advice, significantly lowers the ML/TF risks of the sub-sector.

Somewhat higher risk attaches to a small number (less than 1%) of barristers who are authorised by the Bar Council to provide specialised legal advice directly to clients in the area of trust and tax law under a "direct professional access" scheme which is limited in scope.

Law enforcement intelligence suggests that the exploitation of legal services may occur in respect of high-end or more sophisticated money laundering, involving a wide range of perpetrator types. While there are intelligence gaps in respect of the scale of proceeds being laundered in connection with legal services, the risk of money laundering is heightened by the nature and scale of transactions for which legal services are necessary and also by the fact that legal services providers must serve a wide variety of clients ranging from persons in need of subsidised legal services to corporate clients and high-net worth individuals, who may or may not be politically exposed persons. Similar to credit and financial institutions and other DNFBPs, Irish legal service providers, are obliged by law to assess the ML/TF risks associated with all categories of client, taking into account the nature of their business activities, e.g. cash intensive businesses, construction or real estate transactions, etc.

While the Law Society recommends that solicitors identify all customers and verify their identification using relevant documents, there are indications the CDD policies and procedures for smaller firms and sole practitioners are not always adequate. These observed inadequacies may be due to a reluctance to seek identifying documents from long term clients; the extent of local knowledge solicitors have about their client-base; or due to inadequate staffing levels which may prevent full compliance with AML/CFT obligations. The high number of sole practitioners and single principal firms in Ireland tends to increase the likelihood inadequate AML/CFT procedures.

¹⁶¹ Solicitors Account Regulations 2014, SI 2014/156

¹⁶² Section 2.19, Bar Code of Conduct

STR reporting is low relative to the scale of the legal services sector, the nature of the services provided, the scale of transactions involved and the diversity of the sector's client base. STR statistics for 2015 show that less than 1% of all STRs reported were raised by solicitors.¹⁶³

Notwithstanding the above, evidence suggests that the overall level of compliance observed has improved in recent years, and that the level of compliance for larger firms is generally high.¹⁶⁴

Overall Risk

The overall ML/TF risk in the legal services sector is judged to be **Medium-High**, while the risk for barristers practising in the Law Library is significantly lower than that for solicitors who hold client assets. While awareness of and compliance with AML/CFT obligations has improved across the legal services sector, the nature of services provided by legal professionals, the scale and variety of the their sector and the low level of STR reporting all tend to increase the overall money laundering risk.

Accountancy Services Sector

Overview

External accountants, along with auditors and tax advisors, are all listed as designated persons under Section 25 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 and as such are required to take all of the preventive measures set out in Part 4. External accountants are persons who provide accountancy services to the public irrespective of whether they hold accountancy qualifications or whether they are members of a designated accountancy body.¹⁶⁵ Auditors are persons who are authorised¹⁶⁶ by a recognised accountancy body¹⁶⁷ (RAB) to conduct statutory audits. Tax advisers are persons who provide advice about the tax affairs of another person.¹⁶⁸

There are nine prescribed accountancy bodies (PAB) which regulate the professional conduct of their members in Ireland. These bodies are the designated accountancy bodies for AML/CFT purposes and are also the competent authorities for their members.¹⁶⁹ They are:

- ACCA, the Association of Chartered Certified Accountants;
- AIA, the Association of International Accountants;
- CIMA, the Chartered Institute of Management Accountants;
- CIPFA, the Chartered Institute of Public Finance and Accountancy;
- ICAEW, the Institute of Chartered Accountants in England and Wales;
- ICAI, the Institute of Chartered Accountants in Ireland;
- ICAS, the Institute of Chartered Accountants of Scotland;
- ICPAI, the Institute of Certified Public Accountants in Ireland; and
- IIPA, the Institute of Incorporated Public Accountants.

Of these, six bodies (ACCA, ICAEW, ICAI, ICAS, ICPAI and IIPA) are RABs who authorise persons to conduct statutory audits.

While auditors must be authorised and regulated by one of the six designated accountancy bodies who are RABs, persons providing accountancy services to the public or acting as tax advisers are not required by Irish law to be professionally regulated members of a designated accountancy body. As such, the supervision by the relevant PAB of external accountants and tax advisers who do not carry out audit

¹⁶³ Financial Intelligence Unit, An Garda Síochána

¹⁶⁴ Information provided by the Law Society

¹⁶⁵ Section 24, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

¹⁶⁶ S.I. No. 312/2016 - European Union (Statutory Audits) (Directive 2006/43/EC, as amended by Directive 2014/56/EU, and Regulation (EU) No 537/2014) Regulations 2016, Regulation 37

¹⁶⁷ ACCA, ICAEW, ICAI, ICAS, ICPAI, IPA

¹⁶⁸ Section 24, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

¹⁶⁹ *Ibid* Section 60(2)(b)

services is only conducted where the accountant or tax adviser chooses to become a member of a relevant institution.

Where an external accountant or tax adviser is not a member of a designated accountancy body, the Minister for Justice and Equality is the competent authority for AML/CFT purposes¹⁷⁰ and oversight falls within the remit of the Anti-Money Laundering Compliance Unit, the ‘AMLCU’, of that Department.

The PABs’ regulation of their members is supervised by the Irish Auditing and Accounting Supervisory Authority (IAASA). IAASA has responsibility for supervising how the accountancy bodies regulate and monitor their members¹⁷¹ and for promoting adherence to high professional standards in the auditing and accounting profession.¹⁷²

There are approximately 34,000 regulated accountants in Ireland.¹⁷³ Of those, approximately 3,500 hold practising certificates as external accountants.¹⁷⁴ ICAI, ACCA and ICPAI are the largest designated accountancy bodies amongst practising certificate holders with 51%, 24% and 17% of the population respectively. There are approximated 1,500 statutory audit firms in Ireland.¹⁷⁵

While regulated accountancy service providers are subject to quality review by their respective designated accountancy bodies, there can be differences in how each designated accountancy body monitors its members. These differences arise in the detail requested in annual returns submissions and the frequency and content of on-site inspections. However, common features are that:

- The designated accountancy bodies adopt a risk-based approach to monitoring; and
- Members complete annual returns which provide detailed information to inform this risk-based approach to monitoring.

The designated accountancy bodies take into account a number of potential risk indicators in determining their risk-based supervisory approach. These can include:

- Previous supervisory experience of individual firms;
- Client types;
- Extent of investment business activities;
- Extent of client monies handled;
- Nature of services provided; and
- Extent of internal controls reported.

The Consultative Committee of Accountancy Bodies – Ireland (CCAB-I) - an umbrella group for four of the accountancy professional bodies in Ireland - has published comprehensive AML/CFT guidance¹⁷⁶ for regulated accountants. This guidance highlights to regulated accountancy service providers the obligations, risks and risk indicators specific to the accountancy services sector, in order to raise awareness among their regulated members.

The designated accountancy bodies have observed an overall improvement in awareness and compliance with AML/CFT obligations among their members with a low level of non-compliance detected in recent years. However, the designated accountancy bodies have observed a correlation between irregularities in a firm’s annual return and the presence of AML/CFT inadequacies. Despite the supervisory activity of the designated accountancy bodies over their members, the level of Section 63 reporting by the designated accountancy bodies is low. Section 63(4) of the Act requires competent authorities, such as the PABs, to inform An Garda Síochána and the Revenue Commissioners where they acquire information or

¹⁷⁰ *Ibid* Section 60(2)(e)

¹⁷¹ Sections 904(1)(a), s 905(2)(g) Companies Act 2014

¹⁷² *Ibid* Section 904(1)(b)

¹⁷³ IAASA, Profile of the Profession 2014, p 7

¹⁷⁴ *Ibid* p 16

¹⁷⁵ *Ibid* p 18

¹⁷⁶ CCAB-I, Anti-money laundering guidance for members of the bodies affiliated to the consultative committee of accountancy bodies in Ireland, September 2010

form a suspicion that a person has been or is engaged in money laundering or terrorist financing. Approximately five Section 63 reports were filed by the nine PABs between 2012 and 2015.

Main Vulnerabilities

Similar to the legal services sector, the specialist nature of the knowledge and services provided by the accountancy service providers makes them vulnerable to being sought out and exploited by those who seek to launder the proceeds of crime or evade tax. It is recognised in international risk-based guidance that accountancy service providers may be sought to assist in the structure and design of transactions intended to conceal the nature and origin of funds. Vulnerable services can include:

- Company and trust formations;
- Insolvency services;
- Providing financial advice;
- Providing tax advice;
- Handling client money;
- Managing client assets and financial accounts;
- Investment business services;
- Auditing financial statement; and
- Company secretarial services.

Accountancy service clients – both corporate and individual – come from all areas of commercial activity and inevitably include higher risk clients such as:

- High net worth clients;
- Politically exposed persons; and
- Other known potential higher risk clients for money laundering purposes, e.g. cash intensive businesses, construction or real estate transactions, suspected criminals etc.

The nature of accountancy services is such that they may be used to effect high-end money laundering and there is an awareness, at both national and sectoral level, that accountancy service providers who provide the above services may be at risk of unknowingly facilitating money laundering. This risk may emerge particularly where CDD procedures are too rudimentary to establish sources of funds, or the ultimate beneficial owner of funds involved in what may be complex transactions, which may involve multiple jurisdictions and legal arrangements. Similar to the legal services sector, the involvement of accountancy service providers provide a veneer of legitimacy to illicit transactions and may thereby enable easier access to the legitimate financial sector for entities seeking to launder the proceeds of crime.¹⁷⁷

Entry to the accountancy services market in Ireland is less controlled than is the case for legal services, for example. The term ‘accountant’ is not legally defined, therefore individuals with specialist skills may enter the sector without supervision by the PABs and without immediately coming to the attention of either the AMLCU or the tax authorities. The risk here, which has also been identified in other jurisdictions, is that these non-affiliated service providers may knowingly or unknowingly facilitate the structuring of illicit transactions.

It is difficult to estimate the population of tax advisers and external accountants who are not members of a PAB and consequently fall under the supervisory remit of the AMLCU. It is acknowledged that the AMLCU monitors a small portion of this sector with 120 tax advisers and external accountants currently supervised by the AMLCU. The AMLCU has inspected 79 tax advisers to date. The results of the initial inspections showed that the majority of tax advisers inspected who were in a business relationship with their customers had not identified them and were not fully compliant with their obligations under the Act. Following further inspections they are now aware of their obligations and have complied with the relevant sections of the Act. The AMLCU is aware that there is a number of tax advisers who are not currently being supervised

¹⁷⁷ Including laundering the proceeds of tax evasion

for money laundering and terrorist financing purposes. In order to identify these tax advisers, the AMLCU is in close collaboration with the Revenue Commissioners with a view to obtaining contact details for tax advisers who have registered with the Revenue Commissioners for tax purposes. Innovations in accounting services such as online bookkeeping and online tax-returns services may also increase the vulnerability of the sector as these services tend to be provided on a non-face to face basis and tend also to be provided by unregulated accountancy service providers.

Regulated accountancy service providers do not generally hold client money, but where they do, the monies must be held in a designated client account. Holding client money increases risk but this is mitigated by PAB regulations which require detailed records of client money transactions. As in the legal sector, supervisory visits focus particularly on the management of client funds.

Law enforcement intelligence suggests that the exploitation of the accountancy services sector is more prevalent in respect of high-end and organised money laundering which may involve a wide range of perpetrator types. While there are intelligence gaps in respect of the full scale of proceeds being laundered as a result of involvement of the accountancy services sector, the risk of money laundering due to the nature and scale of transactions associated is high.

STR reporting is low relative to the scale of the accountancy services sector, the nature of the services provided, the scale of transactions involved and the diversity of the sector's client base. STR statistics for 2015 show that less than 1% of all STRs reported were raised by accountancy service providers.¹⁷⁸

Overall Risk

ML and TF risks in the accountancy services sector is mitigated by PABs' AML/CFT supervision, however this mitigating factor is not present for all accountancy services providers and so the sectoral risk assessment is judged to be **Medium-High** on the basis of the nature of the services provided, the scale of the sector and the low level of STR reporting from the sector.

Supervisory evidence indicates that awareness of, and compliance with, AML/CFT obligations has improved among accountancy service providers in recent years.

Non-Profit Organisations

Overview

There are approximately 8,200 registered charities in Ireland. To qualify for charitable status, an organisation must meet certain criteria set out by the Charities Act of 2009. These can be summarised as follows:

- The organisation must be established for the advancement of a charitable purpose;
- The organisation must provide public benefit; and
- All of the property of the organisation must be applied to its charitable purpose.

Although not 'designated persons' for the purposes of AML/CFT legislation, measures have been put in place to mitigate any ML/TF risk in the NPO sector. In October 2014, the Government established the Charities Regulatory Authority (CRA) to regulate the charity sector. At the same time, Ireland's first statutory Register of Charities was published online on the website of the new Authority. It is now mandatory for all charities operating in Ireland to apply to the Authority to be placed on this Register. This Register was created on the basis of pre-existing tax and revenue information held by the Revenue Commissioners and the CRA is engaged in a process of information gathering on these organisations in order to complete their entries on the Register. Not all charities operating in Ireland appear on the Register. It is estimated that the register will grow to an estimated 12,000 organisations by the end of 2016.

As part of the development of its monitoring programme, it is the intention of the CRA to develop a risk-based monitoring framework for registered charities. There may be scope to include money laundering

¹⁷⁸ Financial Intelligence Unit, An Garda Síochána

and terrorist financing risk factors in such a way that would assist with understanding of this risk in Ireland’s charity sector.

Non-Profit Organisations, or ‘NPOs’, whose purposes fall outside of the definition of charitable purpose are not registered or regulated by the Charities Regulatory Authority (CRA). This wider NPO sector includes community and amateur sports organisations; social enterprises; trade unions; political or advocacy organisations; and human rights organisations. FATF’s NPO definition is:

A legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.

As such, there exists a gap between NPOs regulated by the CRA and the wider scope of NPOs under the FATF definition.

There are intelligence gaps in respect of ML/TF in the NPO sector in Ireland. However, there is an increased risk of money laundering in the NPO sector due the developing state of NPO regulation in Ireland, and the potential for NPOs to be unknowingly used to transfer the proceeds of crime to higher risk jurisdictions in which they may operate.

The collection of charitable funds either within community institutions or by charities/NGOs in general raises concern in relation to terrorist financing. Such funds may be collected for the stated reason of supporting humanitarian relief in conflict zones. While there is no evidence to suggest that such funds are being misused, it can be difficult to establish the bona fides of such groups.

Overall Risk

The overall ML/TF risk in the Non-Profit Organisation sector is judged to be **Medium-Low**. This is due to the fact that there is no evidence to date of the abuse of this sector for money laundering or terrorist financing purposes. It is acknowledged that the current picture with regard to the charity sector is incomplete as work is on-going to populate the national register.

Gambling Sector

Overview

There is a wide range of gambling operators in Ireland who provide products and services to many different types of customer. While the majority of gambling operators are unsupervised for AML/CFT purposes, they are otherwise licensed and regulated under the provisions of the Betting Act 1931 (as amended) (‘the Betting Act’) and the Gaming and Lotteries Act 1956. Irish law distinguishes between three main forms of gambling. These are betting, gaming and lotteries. Gambling operators include:

1. Private Members Clubs;
2. Gaming Operators;
3. Lottery Operators; and
4. Betting Operators (retail bookmakers; online bookmakers and betting intermediaries; and on-course bookmakers).

Each of the categories above is explained in further detail below:

1. Private Members Clubs (PMCs)

PMCs are the only category above within the scope of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 and currently subject to regulation for AML/CFT purposes.¹⁷⁹ This section of the National Risk Assessment considers primarily the ML/TF risks associated with other gambling operators outside the scope of the Act. PMCs have been separately considered elsewhere in the National Risk

¹⁷⁹ Section 24, Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

Assessment,¹⁸⁰ due to their regulated status – as such the risks and mitigants pertaining to PMCs will not be discussed in depth in this section.

2. Gaming Operators

Gaming is the playing of a game of skill, chance, or partly skill or chance, for stakes wagered by the player. As such, the definition of gaming covers card games and casino games. The Gaming and Lotteries Act 1956 effectively prohibits the provision of gaming services, although with a confined exception for gaming that occurs in PMCs, which is considered elsewhere in the National Risk Assessment, and gaming halls with gaming machines. At the end of 2015 there were 58 gaming licenses, 6644 gaming machine licenses, and 8137 amusement machine licenses issued in Ireland.¹⁸¹

3. Lottery Operators

Lotteries are also generally prohibited by the Gaming and Lotteries Act 1956 except in certain limited circumstances. The Minister for Public Expenditure and Reform is responsible for the regulation of the National Lottery in accordance with the National Lottery Act 2013. The National Lottery has a dedicated regulator. Charitable lotteries may be permitted by either An Garda Síochána¹⁸² or the District Court.¹⁸³ However, lotteries are not thought to present a risk of money laundering or terrorist financing to Ireland due to the strict regulation of lotteries and the confined circumstances in which lottery permits may be granted.

4. Betting Operators

Betting involves the placing of a wager on the outcome of an event and is regulated by the Betting Act 1931 (as amended). In Ireland, betting operators mainly consists of retail bookmakers, online bookmakers and betting intermediaries, and on-course bookmakers. The Betting (Amendment) Act 2015 brought online bookmakers and betting intermediaries within the scope of the existing licensing regime in Ireland. In addition, the Betting Act prohibits the offering of remote betting and intermediary betting services to customers in Ireland without a licence, whether operators are located within Ireland or in other jurisdictions. The Betting Act also provides for prosecutions *in absentia* where the operators of remote betting or intermediary services do not obtain a licence.

Provisional figures from the Revenue Commissioners indicate that 269 bookmaker's licenses were renewed or issued in 2015,¹⁸⁴ and the Register of Licensed Bookmakers, as of 1st July 2016, indicates there are 305 registered retail and on course bookmakers.¹⁸⁵ As of July 2016 there were 55 current valid remote betting intermediary's licences and remote bookmaker's licences renewed for 2015 - 2017 in Ireland.¹⁸⁶ These consisted of 44 remote bookmaker's licenses and 11 remote betting intermediary licenses.

Retail Bookmakers

While retail bookmakers still constitute the largest share of the betting market, there has been a significant decline in the number of betting shops over the last 10 years, whilst the on-line sector has increased its market share of the business. This is reflected in a decrease in the number of traditional bookmakers' licences issued/renewed in recent years (see figure 2) and also in the reduction in betting duty receipts from €36.4m in 2007 to approximately €27.7m in 2015.¹⁸⁷ This position is consistent with industry figures regarding the decline in the number of retail bookmakers which indicates that the number of bookmakers' shops dropped from 1365 in 2008 to 870 more recently. The most recent figures from Revenue's Register of Bookmaking Offices, as of 1st July 2016, indicate 781 registered bookmaking offices.¹⁸⁸ This also appears to reflect a consolidation in the retail sector, as industry has pointed out that many of the closures were small independent bookmakers, and they expect the numbers to stabilise around current levels.

¹⁸⁰ See Chapter 6 – Non-Financial Sector, 'Private Members' Clubs'

¹⁸¹ Figures provided by Revenue

¹⁸² Section 27, Gaming and Lotteries Act 1956

¹⁸³ *Ibid* Section 28

¹⁸⁴ Figures provided by Revenue

¹⁸⁵ Revenue, Register of Bookmakers @ 01st July 2016, <http://www.revenue.ie/en/tax/excise/index.html>

¹⁸⁶ Revenue Licensed Remote Bookmaking Operations @ 01st July 2016, <http://www.revenue.ie/en/tax/excise/index.html>

¹⁸⁷ Figures provided by Revenue

¹⁸⁸ Revenue, Register of Bookmaking Offices @ 01st July 2016, <http://www.revenue.ie/en/tax/excise/index.html>

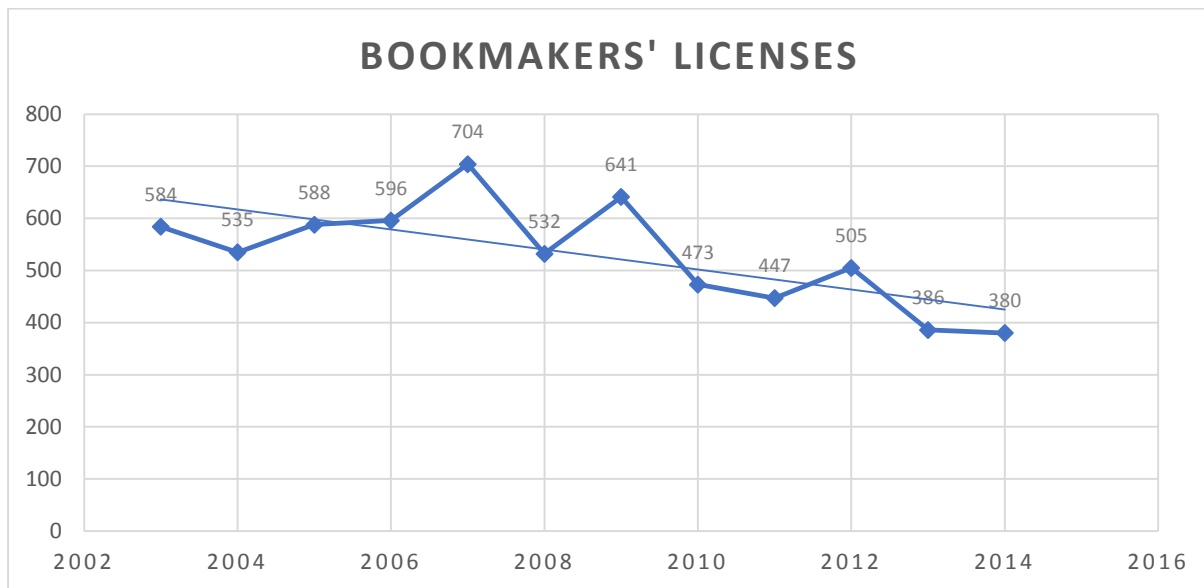


Figure 2: Bookmakers' Licenses Issued / Renewed 2003 – 2014

In spite of its relative decline, the retail sector still represents a significant part of the overall industry and makes a major contribution to the broader economy through employment of approximately 6,000 people.¹⁸⁹ The scale of the sector is reflected in an estimation of its turnover which, based on extrapolation from betting receipts, is concluded to be in the region of €2.61 billion in 2014 and approximately €2.77 billion in 2015.¹⁹⁰ These turnover figures clearly demonstrate a significant sector of the industry, albeit one which has declined in turnover by nearly a quarter in the last decade.

Online bookmakers and betting intermediaries

The online betting sector has grown significantly over the last number of years. This is reflected in the fact that there are 55 online operators now providing betting services in Ireland.

Due however to the fact that the Betting (Amendment) Act, 2015 only extended the existing 1% turnover-based betting duty to remote bookmakers from the latter part of 2015, it has not been possible to accurately compare the scale of on-line sector business with the retail sector up until this year. In this regard, the first quarter 2016 on-line betting duties (€4.5m),¹⁹¹ do give some objective insight into this comparison, and it is estimated that its turnover for 2016 will be in the region of €1.9bn.¹⁹² This would suggest therefore that the online sector represents about 41% of overall turnover in the betting sector.

On-course bookmakers

The betting duty does not apply to this sector, therefore there is little independent information available to estimate its size. However, the industry has indicated that it represents a very small niche area of the betting market and turnover for on-course betting and horse and dog races is in the region of €100m a year.¹⁹³ The Horse Racing Ireland Factbook 2015 broadly corroborates this position, as it indicates that on-course bookmakers took approximately €71 million in bets at horse racing events in 2015.¹⁹⁴

Main Vulnerabilities

The nature of the services and products provided by the gambling sector generate a range of money laundering risks, primarily the opportunity to launder the proceeds of crime, as well as facilitate the

¹⁸⁹ Figures supplied to the AMLSC by industry representatives

¹⁹⁰ Figures provided by Revenue

¹⁹¹ Based on figures provided to the AMLSC by Revenue. In addition, see written answer number 19;

<http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail2016050500040#WRB00700>

¹⁹² i.e. €4.5m x 4 x 100

¹⁹³ Irish Bookmakers Association (IBA) submission to the AMLSC

¹⁹⁴ Horse Racing Ireland Factbook 2015, p 20

spending of proceeds of crime as part of the criminal lifestyle. In addition, there are further risks associated with criminals using the products and service to store or move the proceeds of crime, as well as the possibility of criminals colluding with gambling service providers.

1. Retail and on-course bookmakers

The Industry disaggregates the retail sector into three different tiers. Tier 1 has somewhere in the region of 600 shops, accounts for approximately 80% of market share and employs 5,000 people approximately. Tier 2 has less than 200 shops with 15% of the market share and employs roughly 1,000 people. While Tier 3 has around 90 shops, 5% of the market share and employs about 350 people.

The main vulnerability of the retail sector is the cash based nature of its business. In this regard the industry has confirmed that 97% of traditional betting transactions are placed in cash, although they maintain that the average wager for retail betting is approximately €14, with 90% of all wagers below €25.¹⁹⁵ However, with a high annual turnover in the retail sector, there is undoubtedly significant potential for money laundering if appropriate systems and safeguards are not in place in shops.

Betting operators are not designated persons under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended). Therefore, betting operators are not legally required to perform customer due diligence on their customers for AML/CFT purposes. Due to the lack of a customer identification requirement for the retail and on-course betting sectors there is a significant degree of anonymity which can increase the money laundering risk posed by the cash-based nature of the sectors, allowing masking of the source of the cash.

The extent and effectiveness of transaction monitoring in these sectors is limited by the cash-based and anonymous nature of the traditional betting sectors. In addition, due to the nature of retail and on-course betting, industry argue that it would be difficult to implement AML/CFT customer identification and transaction monitoring measures.

However, the industry argues that retail betting operators actively monitor wagers to detect unusual betting patterns, albeit primarily from a commercial risk perspective rather than an AML/CFT risk perspective. In addition, all bets in the industry are electronically recorded through Electronic Point of Sale (EPOS) systems. They also indicate that approximately 95% of the market share is derived from Tier 1 and Tier 2 operators, who operate a risk-based approach to business and implement staff training for AML.¹⁹⁶ The industry also suggests that comprehensive video monitoring of retail betting premises may reduce this risk by allowing suspicious wagers to be matched to the individuals placing these wagers.¹⁹⁷

Law enforcement intelligence suggests that retail and on-course bookmakers could be vulnerable to exploitation by criminals who place high value wagers in a structured manner to launder significant proceeds of crime. In addition, the transferrable nature of betting receipts could increase the money laundering risk for traditional betting operators. Winning betting slips can be sold by launderers to criminals to launder the proceeds of crime and give criminals an apparently legitimate source of funds.

The diverse customer base of retail and on-course betting operators increases the risk of money laundering, as it has been known to include:

- suspected criminals; and
- Domestic and foreign PEPs.

2. Online bookmakers and betting intermediaries

In contrast to traditional operators, online operators in the Irish market generally require customers to provide identifying documentation when establishing gambling accounts which enables Customer Due Diligence (CDD) to be conducted. This can be for practical purposes, or as these operators often operate in the Irish market from jurisdictions where gambling operators are regulated for AML/CFT purposes, though they are not subject to equivalent regulation in Ireland.

¹⁹⁵ Irish Bookmakers Association (IBA) submission to the AMLSC

¹⁹⁶ *Ibid*

¹⁹⁷ *Ibid*

Due to the nature of the business, online operators accept wagers and winnings predominantly through electronic payment methods. Industry suggests that approximately 95% of all transactions taking place online use credit card, debit cards, or online wallet services.¹⁹⁸ Online operators may also accept e-money, which, depending on the type of e-money service, may not require verification of the source of funds.

However, as a function of their business model, online operators generally implement sophisticated transaction monitoring systems which, due to the extent of CDD conducted, could enable online operators to effectively detect and report suspicious transactions.

Online gaming accounts without turnover requirements are generally considered to be higher risk than accounts with such requirements. A turnover requirement is where account holders are required to wager a certain percentage of any money deposited into an account before being able to withdraw it. Accounts without a turnover requirements could be used as alternative forms of bank accounts existing outside the regulated financial services system. These accounts allow deposits and withdrawals in a manner similar to accounts held at regulated banks without a comparable level of regulation. As such, accounts without turnover requirements are considered to be higher risk. This risk could be further increased where online operators allow cash deposits and withdrawals through their retail branches.

3. Gaming operators

Gaming license holders include gaming arcades and amusement arcades where licensed gaming machines allow gambling to occur. Amusement machines should not allow wagering on any game. In addition, gaming machines, such as “ticket in ticket out” machines, that convert deposited cash into vouchers and can be used as a value transfer mechanism increase the risk of money laundering, as the proceeds of crime could be stored, transferred, and converted back to cash without arousing suspicion of money laundering.

Reporting suspicious transactions

There is a relatively low level of reporting of suspicious transactions in the betting and gaming sectors. A significant factor in this is that operators in these sectors are not within the scope of the relevant legislation and are therefore not under an obligation to report suspicious transactions. They do however report such transactions on a voluntary basis, and there has been an upward trend in such reporting.

Conclusion

An overall risk rating for ML/TF in the gambling sector will not be part of this risk assessment, as work is currently ongoing on a sector-specific risk assessment for this area. Due to the complexity of this area – with various different products and services, along with varied regulatory and licensing regimes – and the requirement to take a risk-based approach to any exemptions from the full scope of the 4th Anti-Money Laundering Directive, this separate risk assessment will be finalised over the coming months in advance of transposition of the 4AMLD. The results of this sector-specific risk assessment, along with the NRA and subsequent Action Plan, will inform policy and legislative developments in this area, and seek to address any vulnerabilities and risks identified through the various risk assessments. For the purpose of clarity, below is a summary of the key issues identified in the gambling sector during this risk assessment, which may inform and be built upon by the subsequent sector-specific assessment.

Retail betting operators are a significant player in this industry and must contend with issues such as the cash intensive nature of their business, which makes them vulnerable to money laundering. This is reinforced by the anonymous nature of transactions, the absence of a legal requirement to verify customer identity and monitor transactions, the scale of the traditional betting sector, and the transferrable nature of betting receipts. Furthermore, there exists a general concern within law enforcement agencies that the system is vulnerable to being exploited by money launderers. A case can be made that these risks are somewhat mitigated by the fact that 95% of the sector is controlled by Tier 1 and Tier 2 operators, who, industry argue, have strong risk-based approaches to how they do business, with risk/trading functions, internal security (loss prevention) teams, operational supervisors, and, in some firms, specific teams reviewing all aspects of AML compliance.

The overall ML/TF risk to on-course operators may be more difficult to assess, due to the nature and relatively small scale of the industry, however is sure to be influenced by factors such as the lack of customer

¹⁹⁸ *Ibid*

identification and the associated anonymity, together with cash intensive nature of this sector. However, the on-course sector accounts for a small proportion of the overall gambling sector.

In the case of online operators the risk rating must take into account both the large and growing scale of the industry, as well as the relative ease in implementing identification and tracking measures into such systems. In terms of scale, the online sector is the fastest growing area of the gambling sector, where the majority of transactions (both wagers and winnings) are through electronic payment methods. Furthermore, as a function of their business model, online operators have a better ability to identify customers, monitor customer transactions and detect suspicious transactions. However the scale of the betting is generally larger.

Whilst the regulated PMC sector is dealt with elsewhere in this NRA,¹⁹⁹ any subsequent sector-specific risk assessment may have to assess both these regulated entities, as well as the amusements and gaming sector which falls outside the classification of PMC.

The overall risk of money laundering and terrorist financing to lotteries in Ireland will reflect the strict regulation of lotteries and the confined circumstances in which lottery permits may be granted. It is not expected that any serious risk exists regarding this section of the industry.

¹⁹⁹ Chapter 6 - Non-Financial Sector, 'Private Members Clubs'

Legal Entities and Arrangements

8

Potential Misuse of Ireland's Legal Entities and Arrangements

In Ireland and elsewhere it is accepted that companies and legal structures (including partnerships, trusts, et cetera) can be used by persons seeking to launder illicit proceeds.

ML/TF risks posed by Irish legal entities and arrangements are neither significantly greater nor lesser than the ML/TF risks posed by similar entities in other developed economies whose legal systems have evolved to facilitate the creation of business vehicles.

A number of factors diminish risks that Irish legal persons and arrangements will be misused for ML or TF:

- The size of the Irish State means its key AML/CFT agencies are unified in nature, a feature that facilitates interaction and collaboration on risk analysis and data sharing between CRO and the Revenue Commissioners as the two key data repositories of corporate information.
- The number of Irish corporate entities is relatively unproblematic from an oversight perspective,²⁰⁰ as Ireland's system is constructed around an efficient 'file and publish' regime which encourages public use and examination of data held in the CRO database.²⁰¹ Open public access to and download of CRO data effectively validates and enhances CRO data in the public arena. CRO also validates data as it is filed and has established an effective system to fine and ultimately strike-off companies which do not file their legal ownership and accounts data annually. Existing measures to gather corporate legal ownership data will soon be complemented by parallel systems to centralise and disseminate beneficial-ownership data as required by EU law;
- The work of Ireland's Office of Corporate Enforcement which disqualifies non-compliant company officers.
- Data interfaces between CRO and Revenue further enhances the transparency of Irish corporates.
- Ireland has achieved the OECD's top compliance-rating in relation to the exchange of tax -related information;²⁰² it is assumed persons considering possible misuses Irish legal persons and vehicles may be discouraged by the fact.
- Ireland is generally an early-adopter of common reporting standards and has demonstrated this in relation to the OECD's Common Reporting Standard (CRS) on financial accounts²⁰³ and on data exchange with the USA in relation to FATCA. Ireland would likely be similarly proactive in relation to the CRS recently proposed for the exchange of beneficial ownership data on legal persons and arrangements; Ireland will implement Articles 30 and 31 of 4AMLD which will require centralised registries of beneficial ownership data on companies in all Member States.

²⁰⁰ Ireland has incorporated approximately 200,000 registered companies, while UK has approximately 3.4 million companies and the Netherlands approximately 2.4 million

²⁰¹ Ireland's online register of companies was visited by 920,000 individual visitors in 2015; 6,375,000 webpages were accessed in 2015 with CRO's search environment being accessed some 700,000 times. CRO promotes access to and re-use of its data by both public agencies and private commercial users such as credit reference agencies and credit and financial institutions

²⁰² OECD, Transparency Ratings, <https://www.oecd.org/tax/transparency/GFratings.pdf>

²⁰³ See Revenue Commissioners, Automatic Exchange of Information, <http://www.revenue.ie/en/business/aeoi/>. Exchanges using CRS for 2016 data due to commence September 2017.

- Through the above measures and as a matter of policy, Ireland is committed to ensuring the transparency of its companies, trusts and other legal arrangements; collaboration between CRO, the Revenue Commissioners and of other key State agencies continues to enhance the accuracy of data held by both the Companies' Registration Office and by the Revenue Commissioners.

Corporate Landscape

At the end of 2015, 198,482 entities were incorporated in Ireland; while some are public limited companies or regulated business subject to sector specific transparency measures, approximately 172,000 of them are small domestic enterprises.²⁰⁴ Incorporation data on of Irish companies (termed 'basic' information by FATF) is held and maintained by CRO. Further data, including beneficial ownership on actively trading 'close'²⁰⁵ companies is held and maintained by the Revenue Commissioners.

In Ireland, all legal persons are registered upon incorporation; the relevant legislation is the Companies Act 2014, and provides for the incorporation of private companies limited by shares (s.17), designated activity companies (s.965), public limited companies (s.1004), companies limited by guarantee, and unlimited companies (s.1231).²⁰⁶

Basic information must be held by the companies themselves at their head offices and by the CRO. The information is publicly available on the company search section of the CRO website,²⁰⁷ or on the registers section of the Central Bank's website.²⁰⁸

Companies

Risk Mitigants

Interfaces have been established between Revenue systems and CRO web services in order to provide the tax authorities with enhanced visibility of company-related data as it is filed. Ongoing nightly interface work gives the tax authorities direct access to company name and status changes as these occur on the companies' register. The interface automatically updates Revenue records, since June 2016, from CRO records so that the tax authorities can systematically identify and contact companies which have not registered for tax with Revenue.

Future interfacing work is planned to assist the CRO, the Office of the Director of Corporate Enforcement and Revenue Commissioners to collaborate and to generate reports on:

- CRO registered companies' status with the Revenue Commissioners;
- Material changes to Irish companies' management and direction, as well as material changes to any major shareholdings in the company.

Control of Companies through Bearer Shares

Clandestine control of Irish companies through bearer shares is no longer possible.

Section 66 the 2014 Companies Act prohibits bearer shares and warrants in the following terms:

“66(8) In subsections (9) and (10) “bearer instrument” means an instrument, in relation to shares of a company, which entitles or purports to entitle the bearer thereof to transfer the shares that are specified in the instrument by delivery of the instrument.

Company shall not have power to issue any bearer instrument.

66(10) If a company purports to issue a bearer instrument, the shares that are specified in the instrument shall be deemed not to have been allotted or issued, and the amount subscribed therefor (and in the case

²⁰⁴ CRO Annual Reports, <https://www.cro.ie/Publications/Publications/Corporate>

²⁰⁵ See Revenue's CT1 Form – question 1.3

²⁰⁶ The Irish Collective Asset-management Vehicles Act, 2015 provides for the incorporation of a very limited number of legal persons called ICAVs - (Section 6) and registration (Section 9)

²⁰⁷ CRO Company Search, <http://search.cro.ie/company/>

²⁰⁸ Central Bank Register, <http://registers.centralbank.ie/DownloadsPage.aspx> : ICAVs are the only corporate vehicles required to register with the CBI and as such the CBI register relates only to the ICAVs. All other companies must register with the CRO

*of a non-cash asset subscribed therefor, the cash value of that asset) shall be due as a debt of the company to the purported subscriber thereof.*²⁰⁹

Overall Risk

The overall risk of money laundering and terrorist financing associated with Irish corporate vehicles is judged to be comparable to or somewhat lower than in other jurisdictions where factors such as larger populations, more extensive geography and federalised systems (i.e. non-unified registries without interfacing to other key data repositories) would tend to heighten risk.

Partnerships

Risk Mitigants

Partnerships in Ireland have a low level of vulnerability to ML/TF abuse, as doing business as a partnership tends to increase levels of both formality and internal/external scrutiny of a partnership-driven business. This occurs by the partners among themselves, by external professionals auditing the partnerships accounts, and by the two main agencies which gather business information, namely the Companies Registration Office and the Revenue Commissioners.

Partnerships occupy a very important place in Irish business life because:

- Firstly, a partnership is a "default" form of business organisation in that whenever two or more people carry on a business venture without forming a company, without necessarily documenting their relations (in a partnership deed et cetera) an "ordinary" partnership arises.
- Secondly, a large section of Irish business is effectively required to use partnerships to operate. Professionals such as lawyers, doctors, dentists, vets and accountants are not allowed to incorporate. Thus at any time two or more such professionals carrying on business together, will invariably be partners.

Some of these terms which arise by statute unless expressly excluded, may not be favourable to the stability and longevity of a partnership. For example, where an ordinary partnership is not based upon a written deed of partnership, the death of a partner causes the partnership to be automatically dissolved, unless a partnership agreement contains provisions to the contrary (1890 Act, Section 33 (1)). Other potentially unfavorable terms of the 1890 Act which are assumed to form part of an undocumented partnership are:

- The assumption that there is no right under a default partnership to expel a partner;
- The right of any single partner in a default/ordinary partnership to dissolve the partnership simply by giving oral notice at a partnership meeting;
- The inability of partners to retire from a default (ordinary/"at-will") partnership, without triggering dissolution of the partnership.

For the reasons set out above, established partnerships in Ireland will typically operate on the basis of a carefully drafted partnership agreement which sets out the rights and obligations of the partners among themselves. Thus, although private in nature, the existence of such partnership agreements, the obligation to register partnerships with the Revenue Commissioners (TR1), the obligation to centrally file partnership names and finally the practical necessity to maintain partnership accounts, effectively means that there is a higher level of transparency and a lower risk of abuse for ML/TF than there would be for in the case of sole traders.

Categories of Partnership in Ireland:

Partnership-at-will, otherwise known as an ordinary partnership, is governed in the absence of any other formal documentation by the Partnership Act, 1890. The 1890 Act is a codification of the common law of partnership as it had developed up to the year 1890. The Act of 1890 does not attempt to provide a complete codification of partnership law however, Section 46 of the act provides that "*the rules of equity*

²⁰⁹ Similar provision relating to public limited companies at Section 1019

and of common law applicable to partnership shall continue in force except so far as they are inconsistent with the express provisions of this Act." Such general partnerships are defined in the first section of the 1890 Act – "partnership is the relation which subsists between persons carrying on a business in common with a view of profit." When business is carried on through the medium of a company, such businesses are specifically excluded from the rules of partnership. It is very important to note that a written partnership agreement is not a pre-requisite for the existence of a partnership, the court has regard to the true contract and intention of the parties appearing from the whole fact of any case that arises.

Limited Partnerships, under the Limited Partnerships Act of 1907, must have at least one general partner and at least one limited partner. The general partner has unlimited liability like a partner in an ordinary partnership, while the limited partners have limited liability since their liability is limited to the amount of capital contributed by them to the firm. The quid pro quo for creating such an entity under the limited partnerships act, is that the limited partners forsake the normal rights of partners to take part in the management of the firm, hence the role of the limited partner is like a shareholder in a limited liability company as their liability is limited to the capital they have contributed. Any ML/TF risk associated with LPs is mitigated as limited partnerships must be registered in the Companies' Registration Office²¹⁰ and can only come into existence on the issue of the certificate of registration by that office. Information Booklet #6 of CRO outlines the significant transparency arrangements in place for such vehicles.²¹¹

Limited partnerships of this type were popular tax-avoidance vehicles during the 1970s; like ordinary partnerships limited partnerships continue to be tax transparent in the sense that they are not taxable as a separate and distinct legal entity, i.e. taxes are levied in relation to the individual partners annually. The key point from an ML/TF point of view is that their attraction as a business form was tax-driven and as such their existence and their accounting was (and continues to be) actively declared to authorities, despite the fact a key tax advantage (ability to reduce limited partners' personal income tax bill against losses) has been eliminated by Revenue. Currently these limited partnerships are principally used as the vehicle of choice for venture capital businesses. From the perspective of AML/CFT, the transparency of such vehicles is relatively high, and the risk of ML/TF is kept relatively low due to the obligation to file information to the central registry.

Partnerships under the Investment Limited Partnerships Act, 1994; the legislation underpinning these vehicles was enacted to encourage the establishment of an International Financial Services Centre in Dublin in the late 80s. It was decided at that time to introduce the concept of a limited partnership to the Irish funds industry because it was noted by Irish authorities that limited partnerships were (and in fact continue to be) popular investment vehicles in the US. Nonetheless, on a statutory basis LLPs are again governed by the general principles of partnership law set out in the Partnership Act, 1890. These statutory forms of partnership are considered to be highly transparent and at low risk of ML/TF abuse because the Central Bank of Ireland regulates their establishment and their ongoing activities. LLPs have a minimum paid-up share capital requirement of €125,000, they must have a general (managing) partner and one or more limited partners and the principal business of LLPs has to be investment. To legally operate these partnerships must secure a certificate of authorisation from the Central Bank.²¹²

Limited liability partnerships of the type now in existence in Great Britain and Northern Ireland have not yet been introduced to Ireland. If and when such entities are provided for in Irish law, it is anticipated that the level of transparency of such vehicles will be reasonably high and the risk of abuse for money-laundering purposes, consequently low. The reason for this assessment is that such limited liability partnerships will essentially be something of a hybrid between company law and partnership law in that they will be separate and distinct bodies corporate, they will be subject to account filing obligations in the same way as companies, and they will be centrally registered and so easily brought within the forthcoming 4AMLD measures to make available beneficial ownership information to obliged entities and law enforcement agencies, including the Revenue Commissioners.

²¹⁰ CRO, Limited Partnerships, <https://www.cro.ie/registration/limited-partnership>

²¹¹ CRO, Information Leaflets, <https://www.cro.ie/Publications-Forms/Publications/Information-Leaflets>

²¹² Analysis of the ML/TF risks associated with entities and arrangements in the Irish funds (collective investment) sector are dealt with in more detail at Chapter 5 – Financial Services Sector

Overall Risk

The overall risk of money laundering and terrorist financing associated with Irish partnerships is judged to be comparable to or somewhat lower than in other jurisdictions where factors such as larger populations, more extensive geography would tend to heighten risk.

Trusts

Risks of misuse of Irish trusts for the purposes of ML or TF are mitigated in Ireland as information on the ownership, control and ultimate objectives of Irish trusts is accessible to law enforcement authorities and to the Revenue Commissioners.

Professional and non-professional trustees in Ireland must maintain records of this nature for a number of reasons:

- Under AML/CFT law, professional trustees in Ireland are ‘designated persons’ (as either legal or accounting service providers, or TCSPs) subject to all preventative requirements of part 4 the Criminal Justice (Money Laundering and Terrorist Financing) Act, 2010. However this designation does not extend to non-professional trustees.
- As a consequence of Irish trust law and precedent for an express trust to be valid under Irish trust law²¹³ one or more instruments or documents (trust deed, associated documents) must provide certainty of intention, certainty of subject matter and certainty of objects. Thus the legal validity requires that the settlor knew what he was doing, the assets under trust are reasonably clear, and the beneficiaries can be identified;
- As a precaution against the possibility of a lawsuit arising in relation to their services within the applicable statute of limitations period;
- To comply with reporting duties imposed upon trustees by Revenue Commissioners in relation to any trust generating tax consequences, including:
 - Registration of the trust if it holds assets under Revenue form TR1;
 - Filing of trust income and chargeable gains under Revenue Form 1;
 - Registration trust if discretionary – Revenue Form DT1;
 - Obligations of trustees to report under Section 896A TCA;
 - Obligations of trustee / executor under form CA24 for Will-trusts;
 - Obligation of trustee to withhold tax and to file Form R185;
 - Reporting regime for *inter-vivos* trusts under Section 817D TCA;

Professional trustees are typically lawyers, accountants, or TCSPs, all of whom are designated persons under the Criminal Justice (Money Laundering and Terrorist Financing) Act, 2010.

Section 55 of the Act requires any designated professional trustee to maintain CDD and transactional records on behalf of the trust for a period of five years after the end of the customer relationship.

Trustees (professional or otherwise) also need to systematically maintain information of this nature so as to present the trust-related information to other designated persons when seeking professional services for the trust. For example, when opening a bank account for the trust, the trustee (professional or not) will be required by any bank to provide information allowing the bank to fulfil its duty to satisfy itself as to the beneficial ownership of the trust under CDD Section 33 (2) and associated Section 28 of the Act.

Future transparency arrangements:

The relevant competent authorities – An Garda Síochána, the FIU and the Revenue Commissioners, have the necessary powers of investigation to compel any information they may require on either companies or trusts; in the near future adequate accurate and current beneficial ownership information will also be available on the main types of legal person as soon as Articles 30 and 31 of 4AMLDD are transposed.

²¹³ Note that footnote 54 of the methodology foresees that trust law countries, like Ireland, may not necessarily have a legislative requirement for criterion 25.1

Overall Risk

The overall risk of money laundering and terrorist financing associated with Irish trusts is judged to be comparable to or somewhat lower than in other jurisdictions where factors such as larger populations, more extensive geography would tend to heighten risk. The Revenue Commissioners' experience in gathering data on trusts generating tax consequences is considered to be a risk mitigant.

Financial Vehicle Corporations (FVCs) and Other Financial Intermediaries (OFIs) including Special Purpose Vehicles (SPVs)

Financial Vehicle Corporations (FVC)

An FVC is an entity whose principal activity meets both of the following criteria:

- it carries out securitisation transactions and its structure is intended to isolate the payment obligations of the undertaking from those of the originator, or the insurance or reinsurance undertaking (in the case of insurance-linked securitisations);
- it issues debt securities, other debt instruments, securitisation fund units, and/or financial derivatives and/or legally or economically owns assets underlying the issue of these financing instruments that are offered for sale to the public or sold on the basis of private placements.

Irish domiciled FVCS have decreased by €98bn or 19% from the period 2011 to 2014 i.e. from €500bn to €402bn at the end of 2014.²¹⁴ Of this figure the National Asset Management Agency (NAMA), a state backed property vehicle, accounts for €75bn. The balance mainly represents FVCs established by credit institutions. In broad terms, FVCs lie outside the regulatory environment, however it should be noted that entities who engage in derivative transactions must report information on their transactions to an approved trade depository under EMIR. FVCs have been obliged to file statistical data to the Central Bank since 2009. They are not currently directly regulated for AML purposes however, those generally responsible for establishing them, i.e. credit institutions, lawyers and accountants have significant ML obligations which goes some way to mitigating the underlying ML/TF risks.

Other Financial Intermediaries (OFIs) including Special Purpose Vehicles (SPVs)

The ECB define OFIs as a corporation or quasi-corporations other than an insurance corporation and pension fund that is engaged mainly in financial intermediation by incurring liabilities in forms other than currency, deposits and/or close substitutes for deposits from institutional entities other than monetary financial institutions (MFIs).²¹⁵ In particular, this includes those engaged primarily in long-term financing, such as corporations engaged in financial leasing, financial vehicle corporations created to be holders of securitised assets, financial holding corporations, dealers in securities and derivatives (when dealing for their own account), venture capital corporations and development capital companies.

The 2015 Financial Stability Board's (FSB) Global Shadow Banking Monitoring Report describes the OFI sector in Ireland as comprising treasury companies, finance leasing companies, holding companies and SPVs that are not primarily engaged in securitization activities.²¹⁶ The overall size of this sector at the end

²¹⁴ FSB Global Shadow Banking Monitoring Report, 2015, p 51, <http://www.fsb.org/wp-content/uploads/global-shadow-banking-monitoring-report-2015.pdf>

²¹⁵ ECB, Financial Intermediaries, <https://www.ecb.europa.eu/mopo/eaec/intermediaries/html/index.en.html>

²¹⁶ FSB Global Shadow Banking Monitoring Report, 2015, <http://www.fsb.org/wp-content/uploads/global-shadow-banking-monitoring-report-2015.pdf>

of 2014 was €498 bn.²¹⁷ In order to get a better breakdown of this area the Central Bank has begun collecting information on the assets and liabilities of SPVs falling outside the FVC definition from Q3 2015. SPV's in general are also outside the regulatory environment and are not regulated directly for AML purposes. However, as with FVCs, there are a considerable number of designated people involved in the creation of such entities such as credit institutions, lawyers, accountants, etc., so this also provides some mitigation of the underlying ML risks.

Conclusion

Most FVCs and OFIs including SPVs are corporate entities. With the transposition of Article 30 and 31 of the 4AMLD, such legal entities will be required to hold details of their beneficial ownership in their books. In addition, this information will be held on a central beneficial ownership register. This will make the ownership of such entities more transparent and will act as a significant ML/TF mitigant. This is an area which will be kept under active review by the AMLSC for developments at both national and international levels.

²¹⁷ *Ibid*, p 51

Cash and other Payment Methods

9

Cash

The use of **cash** for ML and TF purposes is seen as one of the key vulnerabilities by national and international AML and CFT regimes, presenting risks from a transparency perspective, for supervision, and for law enforcement. Cash remains a primary means of transaction across the globe, “[...] with an estimated USD 4 trillion in circulation and between 46% and 82% of all transactions in all countries being conducted in cash”.²¹⁸ Many predicate offences, particularly those traditionally associated with OCGs, ML and TF, generate proceeds of crime primarily in the form of cash – most notably the illicit trade in drugs, counterfeit tobacco, and laundered fuel, as well as many frauds, the sale of stolen goods, and prostitution. Cash can also be used to hamper any attempt to trace the passage of laundered proceeds through the regulated financial sector.²¹⁹ A FATF and MENA FATF report from October 2015, entitled ‘Money Laundering Through the Physical Transportation of Cash’,²²⁰ highlighted many of the issues facing AML regimes regarding the laundering of cash, specifically by cash couriers or smugglers, and pointed out that “[...]cash is still widely used in the criminal economy and it remains the raw material of most criminal activity.”

In addition to the transportation of cash across borders by natural persons, evidence from Ireland, as well as from the UK and the FATF report, suggests that criminals also avail of opportunities to transport cash by way of parcels, cargo and freight.²²¹

There are a number of measures in Ireland to allow for the seizure of the proceeds of crime, or funds which are reasonably suspected of being the proceeds of crime, as discussed elsewhere in this report. Specifically, under Section 39 of the Criminal Justice Act 1994, a Judge of the Circuit Court may order the forfeiture of any cash which has been seized under Section 38 of the Act, if satisfied that the cash directly or indirectly represents the proceeds of crime. Section 38 of the Act authorises the seizure of cash where a member of An Garda Síochána or an officer of Customs and Excise has reasonable grounds for suspecting that the cash (including cash found during a search) represents any person’s proceeds from criminal conduct. The cash seized by a Garda or an officer of Customs and Excise may not be detained for more than 48 hours unless the further detention of the cash is authorised by a Judge of the District Court. Applications can be made to Court to continue to detain the cash for periods of up to two years.²²² The Criminal Assets Bureau, are also empowered to freeze or seize assets which are suspected of being the proceeds of crime. During 2014, the Bureau took proceedings in respect of a variety of asset types with a notable proportion of those in cash/financial type assets, as illustrated below:²²³

²¹⁸ FATF, Money Laundering Through the Physical Transportation of Cash, October 2015, p 3, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html>

²¹⁹ See UK NRA, 8.1

²²⁰ FATF, Money Laundering Through the Physical Transportation of Cash, October 2015, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html>

²²¹ UK NRA 8.16, and FATF, Money Laundering Through the Physical Transportation of Cash, p 28

²²² Information provided by the DPP

²²³ CAB Annual Report 2014, http://www.justice.ie/en/JELR/Pages/Criminal_Assets_Bureau_Annual_Report_2014

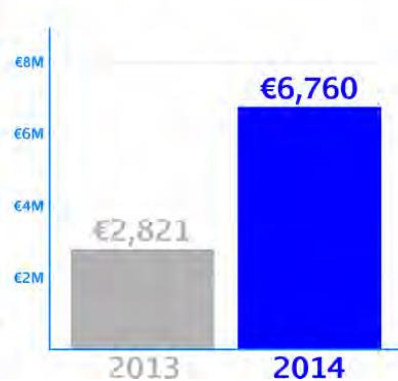
Valuation Breakdown

The value of the twenty two assets frozen under Section 2 of the PoC Act during the year 2014 was €6,760,182. This figure may be broken down in the table below.

Analysis of Section 2 Order by asset type

Description	€
Property	447,000
Jewellery	17,000
Vehicle	76,500
Cash/Financial	6,219,682
Total	6,760,182

Value of assets frozen under Section 2



The Criminal Justice Act 1994 and Proceeds of Crime (Amendment) Act 2005 make provision for Revenue to search for, seize and detain cash found at the point of import or export, if there is a suspicion of a link to criminality. While Revenue investigates the provenance of this cash to establish the link to criminality, such seizures are also advised to the Garda Bureau of Fraud Investigation for the purposes of prosecuting for money-laundering offences, if applicable. Below are figures for cash detentions undertaken by Revenue under Section 38 Criminal Justice Act, 1994.²²⁴ These relate to seizures of cash made by Revenue at ports where there is a suspicion that the funds are the proceeds of crime.

Year	No. Detentions	Amount
2014	38	€906,222
2013	60	€1,341,222
2012	48	€1,191,601
2011	39	€1,029,038
2010	46	€1,693,290

Separately, during 2014, the yield from Revenue audit and compliance intervention programmes increased by 11.3% over the previous year to €610.4 million, with over €196 million of that total coming from sectors where cash transactions are the norm.²²⁵ The Cash Investigations Unit carry out investigations into cash seized under proceeds of crime legislation with a view to establishing a link of the cash to criminality and thereby having the cash forfeit to the State. The experience and success of this unit has resulted in it being regarded as a Centre of Excellence by both the DPP and An Garda Síochána. In any case where there is a suspicion or evidence of money laundering or terrorist financing details are handed over to An Garda Síochána.²²⁶

Proceeds from drug trafficking are generally cash-based and globally, cash remains a significant problem in the fight against money laundering and terrorist financing in a number of sectors. Evidence from the FIU suggests that criminals and third-party money launderers are reluctant to risk using the financial system to launder the proceeds of crime, and gravitate to cash-based channels such as alternative remittance systems or cash couriers/smugglers. If the financial system is utilised, third party money launderers are most likely to be used, as opposed to known criminals, to open bank accounts, credit union accounts or use the services of bureaux de change or payment institutions to transfer funds abroad. An element of ‘smurfing’ might be used – where smaller amounts of cash are lodged/transacted at any given time in an effort not to raise suspicion. Similarly, some businesses may be set up as a ‘front’ purporting to operate as a cash-based business. A business bank account is then opened. This is one area identified by the FIU as being particular vulnerable.²²⁷

²²⁴ Information provided by Revenue

²²⁵ Information provided by Revenue

²²⁶ Information provided by Revenue

²²⁷ Information provided by An Garda Síochána

Irish criminal groups operate on an international basis through countries such as Spain, the Netherlands and the United Kingdom in the importation of controlled drugs into Ireland – cash based operations generally.²²⁸ An Garda Síochána have indicated that the proceeds from many instances of commercial fraud and cybercrime are often relatively quickly withdrawn as cash and laundered further, spent, or deposited in separate accounts, making the funds particularly difficult to trace or recover. The cash based nature of these crimes is reflected in the Transcrime Organised Crime Portfolio (OCP) report of 2015, where their analysis shows that moveable assets, and in particular cash, represents the biggest share of confiscated goods between 2005 and 2012 in Ireland.²²⁹

As mentioned elsewhere in this report, cash remains a key contributor to risk in certain sectors, stemming from a number of factors, including; difficulty in tracing cash; anonymity of cash transactions; transferability of cash; prevalence of cash payments in illicit industries; and the smuggling of cash across international borders. Although the use of the recently discontinued €500 note was not singled out as particularly problematic in the Irish context, the use of high-value notes for the physical smuggling or couriers of cash appears to be significant. The risks inherent in the use of cash reinforce the need for AML and CFT measures in sectors such as HVGDs, cash-based businesses, gambling, and MVTs, amongst others. Many individuals and businesses operating in these sectors, where large amounts of cash may change hands frequently, specifically integrate guidelines and procedures for AML and CFT to deal with circumstances where suspicious transactions involve cash, particularly where certain cash thresholds are met. This includes designated situations, such as in the case of the €15,000 threshold for HVGDs, but also cases such as internal rules within bookkeepers' businesses, or the guidance set out for solicitors in the Law Society Guidance, specifically paragraph 4.15, which highlights the ML risks in cases of payments made by cash.

Some of these issues can be exacerbated due to the existence of a land border with Northern Ireland, and more generally the proximity to the United Kingdom, which enables movement of cash both as euros and pounds sterling between jurisdictions. In addition, certain illicit proceeds generating activities (such as fuel laundering and tobacco smuggling), as well as certain ML channels (such as cash smuggling and Bureaus de Change), are more prevalent in border regions. In April 2014, the FATF team behind the 'Money Laundering Through the Physical Transportation of Cash' report gathered responses from FATF and FSRB members on whether they viewed that ML through physical transportation of cash was increasing, static, declining or fluctuating, and why they thought this was the case.

Two-thirds of the respondents recognised cash smuggling as a significant risk, and of those, half reported that it was an increasing problem. However the remaining third of respondents were unable to assess the scale of the problem in their country.²³⁰

One respondent did state that the practice was declining, and attributed this to improved border controls, leading to increased difficulty for criminals in moving cash across borders undetected, thus leading to a steady decline in the amount of cash seized. However, the one third of countries that said that the problem was increasing, gave a variety of reasons for their answers, all of which are noteworthy for national and international AML and CFT policy, so as to avoid unintended consequences of reform in this area. These reasons included:

An increase in the robustness of banking controls. As AML/CFT measures become more effective and better enforced, criminals find it more difficult to introduce cash into the financial sector, and are forced to physically transport it across borders instead. This was the most common reason cited.

An increase in criminal activity. Some countries perceived that the level of acquisitive crime in their jurisdiction (or a neighbouring jurisdiction) had increased, leading to an increase in the level of criminally derived cash generated.

Lax border controls, or a lack of resources or will to implement border controls effectively. Some countries believe that certain criminal groups have identified that border controls are ineffective in some areas and take advantage of these weaknesses to move cash with little risk of detection.

²²⁸ Savona Ernesto U. & Riccardi Michele (Eds.), 2015, From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Final Report of Project OCP – Organised Crime Portfolio (www.ocportfolio.eu). Trento: Transcrime – Università degli Studi di Trento,

²²⁹ Information provided by An Garda Síochána

²³⁰ FATF, Money Laundering Through the Physical Transportation of Cash, October 2015, p 29, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html>

Economic and/or political instability. In countries where the regular financial system is disrupted due to conflict or serious instability, all types of persons, including those engaged in criminal activity, will seek to move their assets to somewhere safer.²³¹

Conclusion

Ireland's AML/CFT legal framework recognises the risks associated with the use of cash and tries to minimise such risks by requiring designated persons under Article 33 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 to carry out a series of measures such as identifying the customer, and verifying the customer's identity on the basis of prescribed documentation. This is illustrated in that high value good dealers are required to undertake due diligence measures in respect of transactions involving cash of at least €15,000 (whether in one transaction or in a series of transactions). Irish legislation also, as mentioned above, provides for the seizure of the proceeds of crime including cash. These processes by their nature act as a deterrent to the use of cash for ML/TF purposes, however they do not remove it altogether. Consequently, Ireland, like all other countries, continues to be vulnerable to abuses in this area primarily because of the nature and universality of cash transactions. However, both nationally and at EU level, this area will be kept under review.

E-Money

E-Money can be best described as a digital form of cash, since it has many of the characteristics of cash. E-money may be in the form of value stored on a technical device such as a chip card, or on a server. Customers buy the electronic equivalent of fiat currency. The customer, in effect, has exchanged fiat currency for another means of payment. Instead of using a debit or a credit card which requires an account with a credit institution (or other regulated entity), the customer has purchased a non-cash means of payment, which can be used operationally in much the same way as cash or other forms of card payment. Issuers of e-money in Europe are regulated by the E-Money Directive (2009/110/EC),²³² and either need to be registered in an EU Member State as an electronic money institution, or hold a higher-level license, such as a banking license, allowing them to issue e-money.

E-money can therefore be defined²³³ as monetary value as represented by a claim on the issuer, which is:

- electronically stored on an electronic device or remotely at a server,
- issued on receipt of funds for the purposes of making payment transactions, and
- accepted as means of payment by a natural or legal person other than the issuer.

One common type of e-money is the electronic 'e-purse', where users store money on a payment card or other smart card, to use for making payments, often for public transport. E-money can also be stored on (and used via) mobile phones or in an online payment account or 'wallet'. A number of online businesses offer services based on the issuance of e-money, either operating with a banking license or as a licensed e-money institution.

²³¹ *Ibid*

²³² Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

²³³ Per Central Bank website <http://www.centralbank.ie/regulation/industry-sectors/electronic-money-institutions/Pages/default.aspx>

The following are some typical uses of e-money products and services:

- money transmission and payment of bills,
- payment for products or services online,
- tourism and business travel,
- purchasing of gifts,
- pay rewards and incentive programs,
- issuance of store cards,
- multi-vendor shopping centre gift cards, and
- issuance of transport cards.

Provision of E-Money Services

The development and provision of E-Money can involve a number of different parties which can include Issuers, Agents and Distributors.

- An **E-Money Issuer** is an undertaking that has been authorised to issue e-money in accordance with the E-Money Directive²³⁴ An e-money issuer authorised in one Member State within the EU can also passport its services or establish a branch in another Member State under the E-Money Directive
- An **Agent** is a natural or legal person who can provide payment services²³⁵ as well as distribute and/or redeem e-money; e-money agents are not permitted to issue e-money
- A **Distributor** is a natural or legal person who can distribute and/or redeem e-money, but who cannot provide payment services. Distributors may be unregulated and might include businesses such as corner shops or petrol stations that sell prepaid e-money products:

Several or many roles may be performed by the same party, depending on the specific type of e-money product.

The Money Laundering Risk Attaching to E-Money

National law enforcement agencies and international standard-setting bodies, such as the FATF and Moneyval, have pointed to the money laundering and terrorist financing risk associated with e-money, which typically offers a rapid and often anonymous payment option.²³⁶ Since e-money products are used frequently to effect smaller payments, in particular where the product is non-reloadable or benefits from simplified due diligence thresholds, issuer's ability to understand their customers and detect unusual transactions can be limited. Additionally, e-money either on pre-paid cards or in e-wallets can be used by multiple users and the user does not have to be the person who originally obtained the product.

FATF has noted that the absence of credit risk (meaning the service provider may have less incentive to obtain full and accurate information about the customer/business relationship than those service providers who provide credit to their customers), speed of transactions and non-face to face nature of the business are among the common risks associate with payment methods such as e-money²³⁷.

²³⁴ Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions [the 'Directive'] The Directive was transposed into Irish law through the European Communities (Electronic Money) Regulations 2011 (the E-Money Regulations).

²³⁵ Payment services are defined in the Payment Services Directive (Directive 2007/64/EC) and include in this context the placing or withdrawal of monies from a payment account such as operated by an e-money issuer

²³⁶ European Supervisory Authorities 2012 report on the application of AML/CTF obligations to, and the AML/CTF supervision of-money issuers, agents and distributors in Europe, <https://www.eba.europa.eu/documents/10180/16148/JC-2012-086--E-Money-Report---December-2012.pdf>

²³⁷ FATF Report, Money Laundering using New Payment Methods, October 2010, <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

Depending on the type of e-money product, the user may not be required to identify the source of funds used to add value to the e-money product and this increases the risk that the product might be used to launder money or contribute to financing of terrorism as it provides the user with anonymity.

Depending on the nature of a specific e-money product, the characteristics that may increase money laundering and terrorist financing risk may include the following:

- simple accessible nature of the service,
- ability to speedily transfer funds,
- ability to easily move or access e-money (cards or online),
- wide geographical reach and acceptance,
- online service representing a lack of face to face interaction with the customer ,
- facilitates anonymity because identification documents may not be required or verified and source of funds may not be requested,
- loading/reloading and withdrawing by cash offers little or no audit trail,
- funding by unverified parties, whether it is the customer who is unverified or a third party,
- ability of consumers to hold multiple purses (for example open multiple accounts or purchase a number of cards) without verification of identity,
- ability to have high, or no transaction or purse limits particularly where customers are permitted to hold multiple purses, or
- distributors are often not in the financial services industry and offer such services as an ancillary activity to their main business (e.g. retailers, grocery, etc.).

Conclusion

The ML/TF risk associated with e-money has to be acknowledged in an Irish context. However, the imposition of controls or limitations on the value or usage of individual e-money purses or other products can mitigate such risks. Such controls may be by way of legislation. For example, there are obligations to carry out CDD above specified limits set out in legislation.²³⁸ Alternatively, control measures may be introduced internally by the e-money issuer themselves. For example, some e-money products require use of bank accounts or other regulated accounts to load, reload or withdraw monies, which reduces the ML risk associated with using e-money services and products. As such, the inherent risk in this area is mitigated by the relatively low thresholds for exemption from CDD, the requirement to be licensed within the EU to issue e-money, and the necessity of creating a profile for the use of many larger online e-money services. In addition, there has been little indication from law enforcement that e-money is being used for significant amounts of money laundering or terrorist financing, however the nature of such methods may make this hard to detect. This is an area which will be kept under active review at both national and EU level.

Virtual Currencies

Virtual currency can currently be best understood as a digital representation of value that can be digitally traded and function as a medium of exchange, a unit of account, and/or a store of value, but does not have legal tender status in any jurisdiction, and fulfils the above functions only by agreement within the community of users.²³⁹ Virtual currencies could present unique challenges to both regulators and law enforcement agencies, as issues arise regarding both the definition and understanding of virtual currencies and the emerging properties of these markets. As such, few jurisdictions currently regulate virtual currencies

²³⁸ Section 34(d) of the Criminal Justice (Money laundering and Terrorist Financing) Act 2010 provides that for e-money products that cannot be recharged the monetary value that may be stored electronically cannot exceed €250 or if the device cannot be used outside the State than this threshold is €500. For E-Money products that can be recharged, the monetary value cannot exceed €2,500 in any calendar year and no more than €1,000 may be redeemed by the issuer

²³⁹ Adapted from the definition provided in FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, p 4, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

directly, and many law enforcement, monitoring, or risk-assessing measures are hindered by a number of issues, including lack of information, lack of expertise, and/or anonymity or opacity of the market.

The term ‘digital currency’ is often used interchangeably with the term ‘virtual currency’, however this is misleading and best avoided, as money or currency can be stored in a ‘digital’ form, such as e-money, without being a ‘virtual’ currency. E-money, for example, is not a virtual currency, but a digital representation of fiat currency, is legislated for at EU level,²⁴⁰ and is regulated in Ireland by the Central Bank of Ireland, as discussed above. The issuance of e-money is limited to certain cases, such as institutions holding a banking license or e-money license. No such structured regulation currently exists for virtual currencies at EU level or in Ireland. Virtual currency has also been distinguished by the FATF as “[...] *distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.*”²⁴¹ The EBA has defined virtual currencies as a digital representation of value that is issued by neither a central bank nor a public authority, not necessarily attached to a fiat currency, but accepted by natural or legal persons as a means of exchange, and can be transferred, stored or traded electronically.²⁴²

One of the key characteristics of a virtual currency is that it is not tied to a ‘fiat’ or ‘real’ currency, although it may be possible to redeem virtual currency against fiat currency, at variable or fixed exchange rates. Many virtual currencies are what are known as ‘non-convertible’ virtual currencies – currencies which may be utilised within a virtual world or marketplace, but which may not be redeemed against fiat currency. Other, ‘convertible’, virtual currencies can be exchanged with fiat currencies. A FATF report on key definitions and risks for virtual currencies, published in June 2014,²⁴³ defined convertible and non-convertible virtual currencies thus:

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) [...], and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

Another key distinction made by the FATF report is between ‘centralised’ and ‘decentralised’ virtual currencies. Just as the convertibility is of key importance to AML/CFT risk, due to the flexibility of convertible currencies, the centralised or decentralised nature of a virtual currency has significant implications for supervision, regulation, and cooperation with law enforcement agencies.

Centralised Virtual Currencies have a single administrating authority (administrator)—i.e., a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). [...] Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight.

As mentioned above, **cryptocurrencies** are a subset of virtual currencies, which are math-based, decentralised, convertible, and protected by cryptography. They are perhaps the most widely recognised forms of virtual currency - some of the most popular cryptocurrencies (based on market capitalisation)²⁴⁴

²⁴⁰ Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions, which was later transposed into Irish law through the European Communities (Electronic Money) Regulations 2011

²⁴¹ FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, p 4, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

²⁴² Adam Farkas, Executive Director, European Banking Authority, EBA’s work on Virtual Currencies and Cyber Risks, FSC Meeting, Brussels, 17 February 2016

²⁴³ FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

²⁴⁴ Based on figures from <https://coinmarketcap.com/>

include Bitcoin, Litecoin, Dash, Dogecoin, along with other offerings by Ripple Labs, Ethereum, and Voxelus, which utilise cryptocurrencies as part of a wider service infrastructure.

It is understood that there are currently a small number of Bitcoin ATMs in Dublin, which provide the capacity for a customer to exchange cash for bitcoins on-site. Once cash is exchanged for bitcoins, they can relatively easily be converted to other virtual currencies – some of which are less traceable than bitcoin – used to purchase goods or services anonymously (including in Dark Web marketplaces), transferred to other, more legitimate, e-money/digital wallets or online betting wallets, or simply re-converted to cash using online BTC-EUR currency exchanges. This particular issue has previously been subject to research by Europol and the United Nations Office on Drugs and Crime (UNODC).²⁴⁵

It was reiterated by FATF, in their June 2015 guidance for a risk-based approach to virtual currencies,²⁴⁶ that the 2014 Report had indicated in its risk assessment that “[...] at least in the near-term, only convertible VC, which can be used to move value into and out of fiat currencies and the regulated financial system, is likely to present ML/TF risks”.

Conclusion

There are corresponding concerns amongst Irish law enforcement agencies that convertible virtual currencies – particularly cryptocurrencies with a focus on anonymity – may offer criminals untraceable avenues for both money laundering and terrorist financing. However, at present, many of the potential risks do not seem to have materialised in Ireland. Similarly, a report by EUROPOL in January 2016 stated that “[d]espite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement.”²⁴⁷ Nevertheless, it remains unclear to what extent this can be attributed to low criminal or terrorist uptake of these avenues, a lack of suitability for money laundering or terrorist financing, or simply that money laundering or terrorist financing in this area are remaining undetected. This area is being monitored on an ongoing basis at a national law enforcement, state supervisory, and EU level.

²⁴⁵ UNDOC, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, June 2014, https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf

²⁴⁶ FATF, Guidance for a Risk-Based Approach: Virtual Currencies, June 2015, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>

²⁴⁷ EUROPOL, Changes in modus operandi of Islamic State terrorist attacks, 18 January 2016, <https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks>

Terrorist Financing

10

Non-Financial Sectors

Overview

There is a marked overlap between money laundering and terrorist financing – both criminals and terrorists can use similar methods to raise, store and move funds. The vulnerabilities that arise across all sectors for money laundering are, for the most part, similar to the vulnerabilities for terrorist financing.

Terrorist financing can however differ from money laundering in two respects. Firstly, the funds involved in terrorist financing do not necessarily need to be illicit; that is to say, they may not be the proceeds of illegal activities. Secondly, in money laundering it is often the case that the generation of funds may be an end in itself with, for example, the purpose of laundering being to seek to transmit the funds to a legitimate enterprise. In the case of terrorist financing, the end is to support acts of terrorism and for that reason the funds must, for the most part, ultimately be transferred in some way to persons connected with illegal acts.

In general there are three parts to the terrorist financing activity:

1. Generation of funds, through either illicit or licit activities
2. Storage and/or Transmission of funds, and
3. Use of Funds

In terms of scale, the most significant terrorist financing threat in Ireland stems from domestic terrorists rather than international terrorist groups, with little evidence to suggest a significant risk is currently posed by the latter. Both domestic and international terrorist threats are kept under constant review.

While being vigilant for any developments in this area, it is important in informing relevant actors of the nature of risk to communicate clearly the reality of the scale and sophistication of terrorist groups in this regard. The current position is that the level of terrorist financing in the State is of significantly smaller quantum than that of money laundering. It is also important to note that cash is currently considered the most prevalent modality for storage and transfer of funds. In general it is considered that transactions related to terrorist financing are usually smaller than those associated with money laundering and, for that reason, may not be as easily detected in the context of the high volumes of transactions.

With regards to the use of funding it is also important to note that terrorist financing should not only be seen in the context of financing direct acts of terrorism. Such funding can also be used to establish or maintain terrorist groups and sustain the networks that may connect them. Such funding can support non-violent or obvious aspects of a group's operations by paying for daily living expenses, travel, training, propaganda activities or organisational costs.

Nature of Terrorist Threat

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current available intelligence (general and specific), knowledge of terrorist intentions and capabilities, the timescale for an attack and events outside the State, particularly in neighbouring states, but also in the wider international arena.

Domestic

Republican Paramilitary Groups (sometimes referred to as 'dissident groups') represent the main terrorist threat to the security of the State. While the Good Friday Agreement has delivered a stable peace process that commands overwhelming cross-community support, certain groups in both communities, with very limited levels of support, remain intent on disrupting the progress which has been achieved.

While the most significant grouping involved in Northern Ireland related terrorism declared a ceasefire in 1997, the Peace Process which followed the ceasefire did not enjoy total support from those involved in violent activity. Some terrorist organisations continued their activities and there was also the emergence of new terrorist grouping formations.

It is important to understand that these groups operate on a 'whole of island' basis, with activities occurring on both sides of the border. While logistical support, planning and financing may occur in both jurisdictions, these groups do not generally have as an objective the carrying out of acts of terrorism in this State. For that reason it is generally assessed that an attack in Ireland from this source is unlikely. However, the threat level in Northern Ireland is considered to be 'severe' and in Great Britain to be 'substantial'.

As outlined above, Northern Ireland faces the greatest security threat from this source with the current threat level ranked as 'severe' meaning that an attack is highly likely with members of the security services being the most likely targets. It is not considered that an attack is likely in Ireland but this State is used by these groups for planning and logistical purposes with a view to effecting attacks in Northern Ireland, though domestic terrorists are also involved in a range of criminal enterprises in this jurisdiction.

There are a number of Republican Paramilitary Groups with varying strength and capability and posing varying levels of threat. Some groups are considered to be continually operationally active and are assessed as having been responsible for a number of murders and bomb attacks in Northern Ireland; others are assessed as being active, but in a more sporadic manner. It is important also to understand the potential linkages between Republican Paramilitary Groups and Organised Crime Gangs in the State. A relationship of friction and facilitation exists between Organised Crime Gangs and some Domestic Terrorist Groupings. "Taxing"/extortion of drug dealers by Republican Paramilitary Groups continues to be an avenue of fundraising. Distinguishing the activities of such groupings from Organised Crime Gangs can also be complex, with domestic terrorist groups often acting in an identical manner to Organised Crime Gangs. This can be seen through means by which such groups may at times finance their activities e.g. smuggling, extortion, drugs, etc. and the means by which such funds are concealed.

International

Terrorist attacks across Europe and elsewhere, have brought into sharp focus the continuing serious and dynamic nature of the threat posed by international terrorism against the background, particularly, of continued instability in the Middle East. The phenomenon of individuals travelling from all over Europe to conflict zones is a significant issue of concern to the majority of European states and others internationally. The majority of the current threats to European states and interests are linked to the conflicts in Iraq and Syria, with the major security concerns relating to the radicalising influences that travellers to conflict zones are exposed to and the security risks some individuals may pose on returning to their home countries.

While full cognisance is taken of the events happening internationally, it must be stressed that the threat to Ireland is not assessed to be comparable to that which exists in other European jurisdictions. It is currently assessed that an attack in Ireland from this source is moderate. In other words Ireland enjoys a relatively benign security environment, with no specific intelligence of a particular threat, but that a potential threat may exist.

The threat from international terrorism is kept under constant review by an Garda Síochána, who take into account a range of considerations, including developments in the international threat landscape. In respect of the current threat from international terrorism key considerations include:

- The threat posed by returning fighters from conflict zones;
- Potential for 'Lone Actors' to carry out an attack as demonstrated by recent incidents;
- The increasingly aggressive stance, the terrorist operations and the radicalising potential, of the Islamist terrorist group styling itself the 'Islamic State (IS)';
- Unforeseen "Trigger Events" which might motivate isolated attacks in this jurisdiction;
- Ireland's close relationship with the US, Europe and particularly UK, with whom Ireland shares a common travel area – the current threat level in the UK is 'severe', that is to say, an attack is highly likely.

An Garda Síochána enjoys a very positive relationship with the communities in Ireland in which individuals may be considered to be vulnerable to being radicalised or recruited for international terrorism. This relationship has been developed through community engagement over a long number of years. However, a very small number of individuals have travelled to areas of conflict and returned to this jurisdiction and a number of individuals have been fatally injured in the areas of conflict.

There is also the possibility, albeit currently assessed to be low, that Ireland could be used as a base from which attacks could be planned, etc. Such incidents would be likely to cause extreme disruption in the short-term and possibly longer-term reputational damage to Ireland as a safe and secure destination.

Nature and Degree of Terrorist Financing Threat

It is important to note that the intelligence picture indicates that the financing of terrorism, particularly international terrorism, in this State is not significant when compared to other European states.

Domestic

The costs associated with domestic terrorist acts are, for the most part relatively small. The material used in such acts can be procured often through theft; though certain more sophisticated material may have to be procured through purchase requiring access to funding.

The primary means by which these groups fund their activities is through a range of criminal activities including smuggling, extortion, robberies and the taxing of criminals involved in activities such as organised prostitution, drug trade, etc. Counterfeiting has also more recently been used by some groups. These funds can then be laundered through cash enterprise such as licensed premises and security companies or in the form of 'loans' to businesses fronted by persons with no obvious affiliations to these groups.

The significant success of An Garda Síochána over the years has significantly degraded the capacity of Republican Paramilitary Groups to finance their operations and it is considered that such groups do not have significant reserves, relying on ongoing activities for funding.

International

Ireland is not subject to the same levels of concern regarding the financing of international terrorist activity due to the fact that the numbers of supporters of international terrorism in the State is small when compared with other European jurisdictions, with little evidence to show any coordinated approach to fundraising in support of international terrorism. Intelligence suggests that there is no real 'infrastructure' in place to facilitate fundraising for international terrorism at any significant levels.

International Terrorist Groups through publications on social media etc. provide advice that travellers to conflict zones require little money to participate. While they do advise on the purchase of certain type of personal equipment and clothing, these costs are minimal and, for the most part, intelligence indicates that such individuals fund their own travel.

Notwithstanding the assessed low level of threat posed by financing for international terrorism in the State, there are a number of areas of concern. One such area is the collection of charitable funds either within community institutions or by charities/NGOs in general. Such funds may be collected for the stated reason of supporting humanitarian relief in conflict zones. While there is no evidence to suggest that such funds are being misused, it can be difficult to establish the bona fides of such groups. Similarly while the use of credit cards near conflict zones or the transfer of funds through accounts to such regions are indicators of terrorist financing it must be borne in mind that there are a number of individuals in the State who legitimately send funds to their countries of origin on a regular basis. Appropriate attention is devoted to these cases as necessary.

Nature of Response

An Garda Síochána is a dual mandate organisation performing both a policing and security service role. In its role as a security service An Garda Síochána is very much cognisant of the issue of terrorist financing. An Garda Síochána is aware of the measures in place to detect, disrupt and prosecute offences committed in this area and is taking effective action in combating this problem. This is primarily achieved through

close co-operation between three Sections of An Garda Síochána, namely, Security & Intelligence Section, the Financial Intelligence Unit, and the Special Detective Unit.

Ireland's unitary, centralised policing and security service allows it to effectively investigate all types of crime, including terrorist financing. An Garda Síochána is in continuous contact with relevant stakeholders, such as the Revenue Commissioners, sharing intelligence as appropriate with the relevant sectors, i.e. banks, charities, Property Services Regulatory Authority, etc. to assist them mitigate the risks in respect of both ML and TF.

As outlined above, within An Garda Síochána there are a number of specialist units with particular investigative expertise in the spheres of ML and TF. The Garda Bureau of Fraud Investigation is a specialist bureau that investigates fraud-related crime. The Bureau investigates serious and complex cases of commercial fraud, cheque and payment card fraud, counterfeit currency, money laundering, computer crime and breaches of the Companies Acts and the Competition Act. Located within the GBFI is the Financial Intelligence Unit. The FIU receives, assesses and disseminates Suspicious Transaction Reports from 'designated persons' and reports of suspected Money Laundering and Terrorist Financing from 'competent authorities' such as the Central Bank and the Anti-Money Laundering Compliance Unit amongst others. FIU is in regular receipt of suspicious transaction reports from the banking sector in relation to suspicious transactions. The FIU liaises with the Intelligence Office at Security & Intelligence Section concerning the entities involved in these transactions.

There is regular interaction and exchanges between the FIU and the Security and Intelligence Section concerning entities that come to the attention of the FIU during the course of their business. Similarly, Security and Intelligence Section frequently comes into possession of intelligence relating to bank accounts and transactions connected to persons of interest. The Intelligence Office liaises with the FIU in order to enhance the intelligence picture of these entities and potentially identify areas for further investigation.

Unlawful organisations which pose a threat to the security of the State are investigated by the Special Detective Unit of An Garda Síochána who liaise closely with the Financial Intelligence Unit, also located within An Garda Síochána, who provide intelligence gathered from STRs in addition to identifying accounts suspected of being used by terrorist organisations for money laundering and terrorist financing.